Business Process Model Approach for Management of Plant Alarm System

Kazuhiro TAKEDA[1], Takashi HAMAGUCHI[2] , Naoki KIMURA[3] and Masaru NODA[4]

[1] Graduate School of Engineering, Shizuoka University, 3-5-1 Johoku Hamamatsu, 432–8561, Japan
[2] Graduate School of Engineering, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, 466–8555, Japan
[3] Faculty of Engineering, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka, 819–0395, Japan
[4] Department of Chemical Engineering, Fukuoka University, 8-19-1 Nanakuma, Jonan-ku, Fukuoka, 814–0180, Japan
Correspondence concerning this article should be addressed to K. Takeda (E-mail address: tktaked@ipc.shizuoka.ac.jp).
Presented at the 5th World Conference of Safety of Oil and Gas Industry (WCOGI2014) at Okayama, June 2014

Keywords: Plant Alarm System Management, Plant Lifecycle Engineering, Business Process Model

A plant alarm system is one of the most important elements of the third layer of independent protection layers (IPLs). Management of the plant alarm system has become identified as one of the key issues because of the disasters caused by alarm floods. The instrumentation, systems, and automation society has proposed an alarm management standard. However, an explicit definition of a business process to properly manage the plant alarm system has not been proposed. A plant alarm system is not always designed using the overall information about the plant, because the concreteness and quantity of the information varies along with the stages of the plant design. The requirements for a safety instrumented system may not be satisfied if the design of the plant alarm system was started after all of the stages of the plant design had been completed. The stages of the plant alarm system design should be carried out concurrently with the stages of the plant design. Therefore, the design process of the plant alarm system should be clarified corresponding to the available information at each stage of the design. To clarify the business process concerned with the plant alarm system, a framework is necessary to express the activities with tools, available information and output. Therefore, a business process model (BPM) as the framework for the plant alarm system will be developed. In this paper, we try to express a BPM concerned with a plant alarm system. Even if the developed BPM is incomplete, the BPM approach will have following merits: design rationale for the plant alarm system can be specified and stored, and the plant alarm system can be designed more logically. The stored design rationale and the logically designed plant alarm system are very useful for management of the change of the plant alarm system and ensuring consistency with other safety instruments.

Introduction

Chemical plants must remain in safe states, because the plants treat hazardous and/or toxic materials, and/or are operated at high pressure and/or at high temperature. For plant safety, alarms alert operators of the abnormal states of plants. The alarms are process alarms for the product quality and critical alarms for plant safety. The present paper targets the critical alarms. Chemical plants have been required to be protected from accidents or disasters by independent protection layers (IPLs) (Center for Chemical Process Safety, 2001) as shown in **Figure 1**. The plant alarm system is one of the most important elements of the third layer of the IPLs. The plant alarm system should be managed and maintained through the plant lifecycle. The Instrumentation, Systems, and Automation Society (ISA) (2009) has proposed an alarm management standard. As shown in **Figure 2**, the standard proposes three loops: a monitoring and maintenance loop, a monitoring and management of change loop and an audit of philosophy loop. The standard refers to activities and input-output information of the activities about the alarm system. However there are few descriptions the other activities and information concerned with the alarm system. To perform activities adequately, the activities concerned with the plant alarm system in the plant lifecycle and information flows among the activities should be explicitly expressed as a Business Process Model (BPM). The present paper proposes a BPM concerned with the plant alarm system in the plant lifecycle.

Fuchino *et al.* (2010) extended the Process Industry Executive for archiving Business Advantage using Standards for data Exchange (PIEBASE) model (1998) and proposed a Plan, Do, Check and Act + Provide Resources (PDCA+P.R.) template. Shimada *et al.* (2012) proposed a BPM of Plant Lifecycle Engineering (Plant-LCE) based on the template. Fuchino *et al.* (2010) proposed an overview template to overview the overall BPM. The plant alarm system should be properly managed in the plant lifecycle. Therefore, the proposed BPM is based on the BPM of Plant-LCE, and an overview template of the BPM is based on the overview template proposed by Fuchino *et al.* (2010).

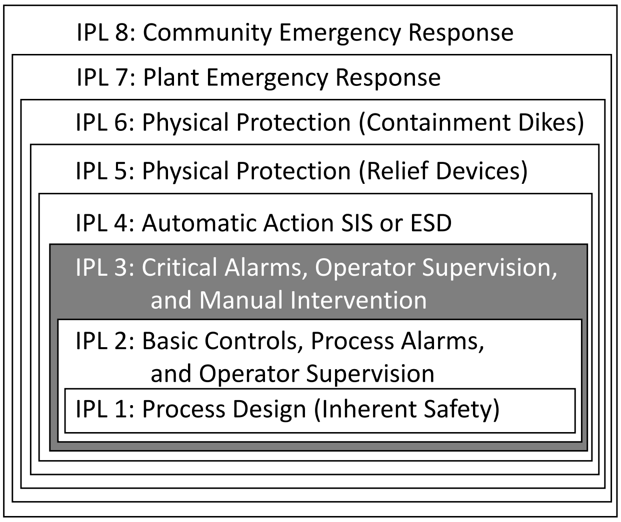


Fig. 1 Independent protection layers

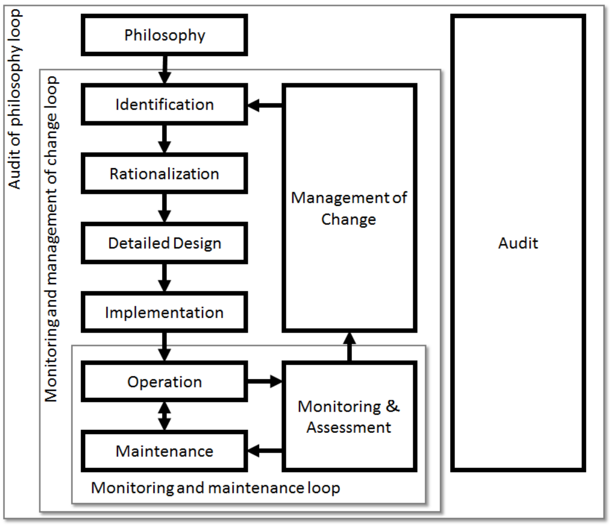


Fig. 2 Alarm management lifecycle

1. BPM for Plant Alarm System Management

Some methods of alarm limit setting or nuisance alarm reduction obtained through the plant improvement activities have been proposed. However, an explicit definition of a business process to properly manage the plant alarm system has not been proposed. A plant alarm system is not always designed using the overall information about the plant, because the concreteness and quantity of information varies along with the stages of the plant design. The requirements for the safety instrumented system may not be satisfied if the design of the plant alarm system was started after all stages of the plant design had been completed. The stages of the plant alarm system design should be carried out concurrently with the stages of the plant design. Therefore, a design process of the plant alarm system should be clarified corresponding to the available information at each stage of the design. Furthermore, problems about the plant alarm system occurred in operation and/or maintenance should be corrected in the design stages. The plant alarm system should be properly managed through the plant lifecycle. Therefore, a business process concerned with the plant alarm system in the plant lifecycle should be explicitly expressed. To clarify the business process concerned with the plant alarm system, a framework is necessary to express the activities with tools, available information and output. Therefore, a BPM as the framework for the plant alarm system will be developed. In the present paper, we try to express a BPM concerned with the plant alarm system.

1.1 Template of BPM

Process Industries STandard for the Exchange of Product model data consortium (PI STEP) standardizes a plant structure. In the PI STEP, Integrated definition for functional model standard, type-zero (IDEF0) (National Institute of Standards and Technology, 1993) is used as an activity modeling method and PIEBASE model (1998) is used as a framework. Fuchino *et al.* (2010) extended the PIEBASE model and proposed a PDCA+P.R. template. Shimada *et al.* (2012) proposed a BPM of Plant-LCE based on the template. Fuchino *et al.* (2010) proposed an overview template to overview the overall BPM. In the present paper, a BPM concerned with the plant alarm system in the plant lifecycle is based on the BPM of Plant-LCE, and an overview template of the BPM (**Figure 3**) is based on the overview template proposed by Fuchino *et al.* (2010).

In the template of the BPM as shown in Figure 3, an activity is a box and information is an arrow. The arrows into left, top and bottom of a box are 'input', 'control' and 'mechanism', respectively. An out arrow from the right of a box is 'output'. 'Mechanism' arrows are eliminated to simplify. Activities are hierarchically constructed. Expanded activities of an activity are called as nodes. These activities are 'Manage (Act)', 'Plan', 'Do', 'Check (Evaluate)' and 'Provide Resources'. The 'Do' activities may be two or more activities. The request arrows from 'Manage (Act)' activity to 'Provide Resources' activity and the resource arrows from 'Provide Resources' activity to 'Manage (Act)' activity are eliminated to simplify. The outputs from the activity A1 to the activity A6 connects to the next activities, although the outputs are stored in the activity A7 and provided to the next activities. The arrows through 'Check (Evaluate)' and 'Provide Resources' activities contain the same information to simplify, although these arrows respectively contain checked and logged information. The arrows u1, u2 and u3 in the upper activity are respectively the arrows 1, 3 and 8 in the node.

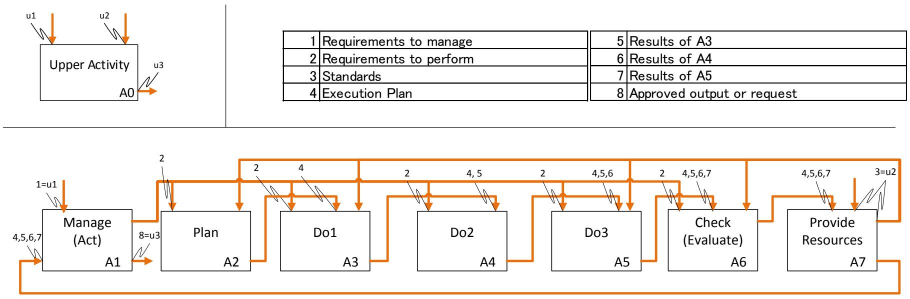


Fig. 3 Template of business process model

1.2 BPM concerned with plant alarm system

The proposed BPM contains activities concerned with a plant alarm system, but does not contain all of the activities of Plant-LCE. In a narrow sense, the activities of a plant alarm system design are under the activity A44563 in **Figure 4 (9)**. However, information about sensors and the control limits for steady state is very important for the plant alarm system design. Further, the design concept of the plant alarm system as a third layer of IPL should be decided as part of the design concept of IPL which handles steady state, abnormal situations and emergency shutdown. Furthermore, redesign for improvement requirements from operation or maintenance should be considered. Therefore, a BPM concerned with the plant alarm system contains activities through the Plant-LCE.

As shown in **Figure 4 (1)**, the activity A1 'Manage Plant-LCE' receives requirements '1=u1' to manage and requires to perform from the activity A2 to the activity A6. The activity A2 'Make execution plan for Plant-LCE' receives the request and makes execution plans. The activity A4 'Perform process and plant design' receives the plan and designs the process and the plant design. The activity A5 'Perform construction' constructs the plant following the design. The activity A5 'Perform manufacturing' manufactures with the constructed plant.

As shown in **Figure 4 (3)**, the activity A6 'Perform manufacturing' contains the activities A62 'Make production plan', A63 'Perform production' and A64 'Perform maintenance'. Improvement requirements for the plant alarm system performance are reported to the activity A65 'Evaluate performance of manufacturing', checked by the activity A65, logged in the activity A66 'Provide resources for manufacturing' and reported to the activity A61 'Manage manufacturing'. If the requirements can be treated by maintenance, the activity A61 requires the activity A64 to maintain the plant alarm system. This loop is the monitoring and maintenance loop of the plant alarm management lifecycle proposed by ISA. If the requirements cannot be treated by maintenance, the activity A61 requests to upper level activities as the arrow '8=(1)-7'. The requirements are checked by the activity A8, logged in the activity A9 and reported to the activity A1. If the activity A1 decides as needing design assessment for the requirements, the activity A1 requires the activity A3 to perform design assessment. Activities for the design assessment are the same activities for ordinary design process. The loop is the monitoring and management of the change loop of the plant alarm management lifecycle proposed by ISA. The audit and philosophy loop of the plant alarm management lifecycle proposed by ISA is a loop to revise philosophy in the upper level activities of the activity A0 'Perform Plant-LCE'.

In the node A4 in **Figure 4 (2)**, the overall operational design philosophy is planned and designed in the first step. Following the philosophy, the process and plant are designed. In lower nodes, the design concepts for the nodes are planned and designed in the first step. Further, following the concepts, the process and plant are designed. These manners for design can ease management of the change of the plant alarm system. In this node, design processes are conceptual, process, preliminary plant, final process, and final plant. In the preliminary process design, the requirements for the plant alarm system design are mostly developed. Therefore, the activity A44 'Develop preliminary process design' is expanded.

In the node A44 in **Figure 4 (4)**, the activity A443 'Develop preliminary process design for normal steady state' designs for normal steady state, and the activity A444 'Develop preliminary process design for normal unsteady state' designs for normal unsteady state. In these activities, the processes for normal steady and unsteady state, the control structures and limits are designed. Using these design results, processes for abnormal situations and emergency shutdown are designed in the activity A445 'Develop preliminary process design for abnormal situations' and the activity A446 'Develop preliminary process design for emergency shutdown', respectively.

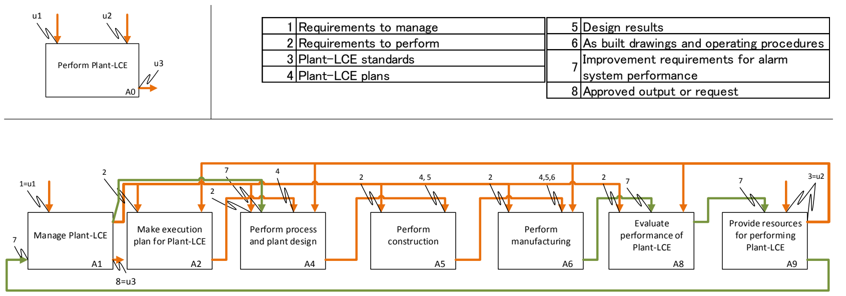
In the node A445 in **Figure 4 (5)**, the activity A4453 'Allocate abnormal situations to IPL' allocates abnormal situations to IPL. If necessary, the activity A4454 'Develop backup process design for abnormal situations' designs a backup process for abnormal situations. The activities A4456 'Develop preliminary process design for IPL3' and A4457 'Develop preliminary process design for IPL4' design preliminary process for IPL3 and IPL4, respectively.

In the node A4453 in **Figure 4 (6)**, the activity A44533 'Perform PHA' performs process hazard analysis (PHA). The activity A44534 'Develop countermeasures for assumed possible malfunctions' designs countermeasures for assumed possible malfunctions in the plant. The activity A44535 'Develop options of abnormal situations allocating to IPL' allocates the abnormal situations to IPLs.

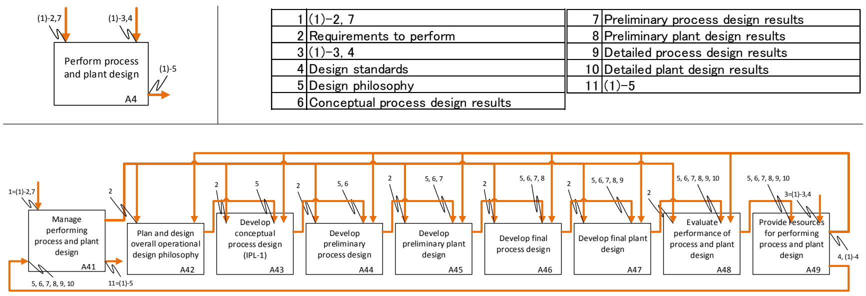
In the node A4456 in **Figure 4 (7)**, the activity A44563 'Develop detailed design for plant alarm system' designs the plant alarm system. The activity A44564 'Develop detailed design for fault diagnosis system' designs the plant fault diagnosis system. The activity A44565 'Develop countermeasures corresponding to the plant alarm system' develops countermeasures.

In the node A44533 in **Figure 4 (8)**, the activity A445333 'Assume possible malfunctions' assumes possible malfunctions in the plant. The activity A445334 'Develop propagation paths assumed possible malfunctions' develops propagation paths from assumed possible malfunctions.

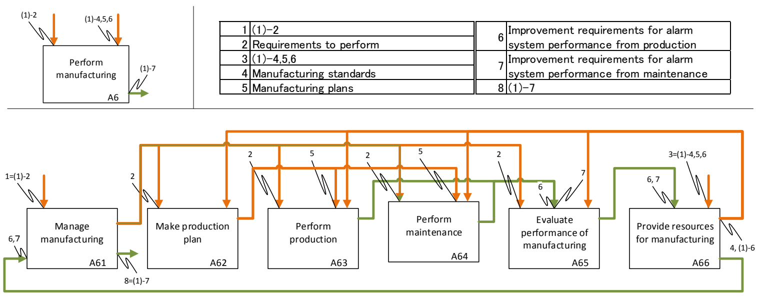
In the node A44563 in Figure 4 (9), the activity A445633 'Develop alarm source signals' selects or newly designs alarm source signals. The activity A445634 'Develop alarm limits' develops alarm limits for the alarm source signals. The activity A445635 'Develop alarm algorithms' develops alarm algorithms. This node contains main activities for the plant alarm system design process. Furthermore, explicitly describing the structure of activities which generate the information using the BPM, design rationale for the plant alarm system can be specified. Further, the plant alarm system can be designed logically.



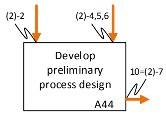
(1) A0 (Perform Plant-LCE) node



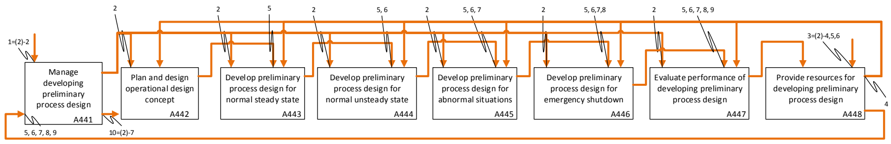
(2) A4 (Perform process and plant design) node



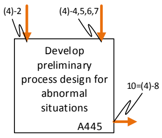
(3) A6 (Perform manufacturing) node



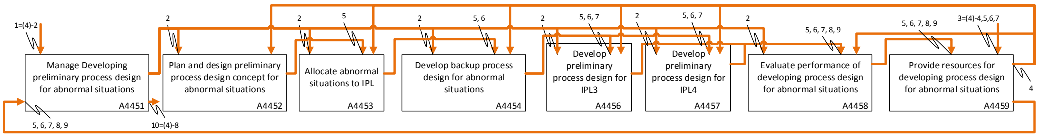
1	(2)−2	7	Preliminary process design results for normal unsteady state operations
2	Requirements to perform	8	Preliminary process design results for abnormal situations
3	(2)−4, 5, 6	9	Preliminary process design results for emargency shutdown
4	Preliminary process design standards,(2)−5,6	10	(2)−7
5	Preliminary process design concepts		
6	Preliminary process design results for normal steady state operations		



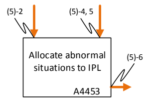
(4) A44 (Develop preliminary process design) node



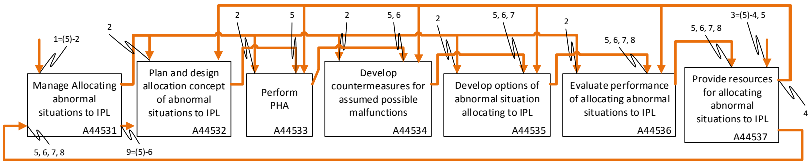
1	(4)−2	6	Allocation of abnormal situations to IPL
2	Requirements to perform	7	Additional processes
3	(4)−4, 5, 6, 7	8	Preliminary process design for IPL3
4	Standards for preliminary prcess design for abnormal situations, (4)−5, 6, 7	9	Preliminary process design for IPL4
5	Preliminary process design concepts for abnormal situations	10	(4)−8



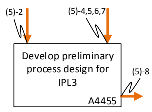
(5) A445 (Develop preliminary process design for abnormal situations) node



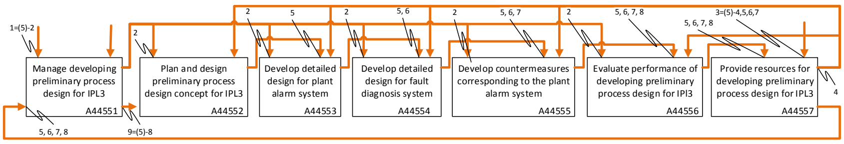
1	(5)−2	6	PHA results
2	Requirements to perform	7	Countermeasure operations
3	(5)−4, 5	8	Options of abnormal situation allocating to IPL
4	Standards for Allocating abnormal situations to IPL, (5)−5	9	(5)−6
5	Allocation concepts ofabnormal situations to IPL		



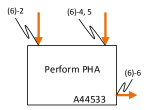
(6) A4453 (Allocate abnormal situations to IPL) node



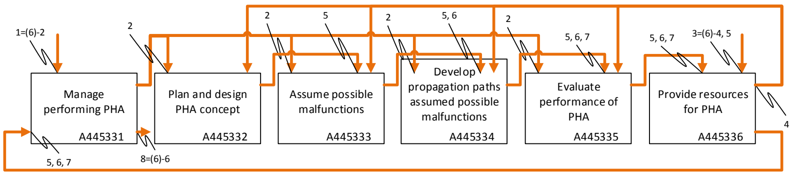
1	(5)−2	6	Detailed design for plant alarm system
2	Requirements to perform	7	Detailed design for fault diagnosis system
3	(5)−4, 5, 6, 7	8	Countermeasures corresponding to the plant alarm sytem
4	Standards for preliminary process design for IPL3, (5)−5, 6, 7	9	(7)−8
5	Preliminary process design concepts for IPL3		



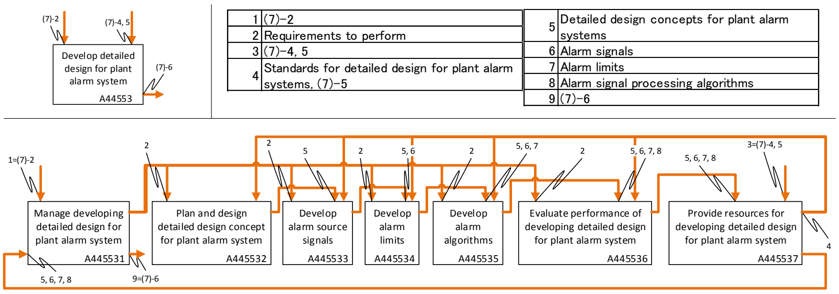
(7) A4456 (Develop preliminary process design for IPL3) node



1	(6)−2	5	PHA concepts for preliminary process design
2	Requirements to perform	6	Assumed malfunctions
3	(6)−4, 5	7	Propagation paths
4	Standards for PHA, (6)−5	8	(6)−6



(8) A44533 (Perform PHA) node



(9) A44563 (Develop detailed design for plant alarm system) node

Fig. 4 Business process model concerned with plant alarm system design process

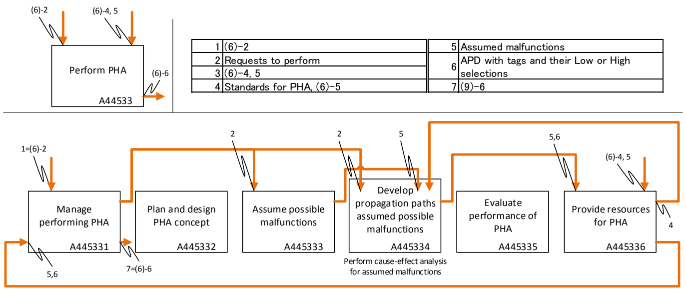
2. Business Flow of Luo Method

The business flow of the Luo method to design a plant alarm system (Luo *et al.*, 2007) was traced on the proposed BPM. The design procedures of Luo method are as follows;

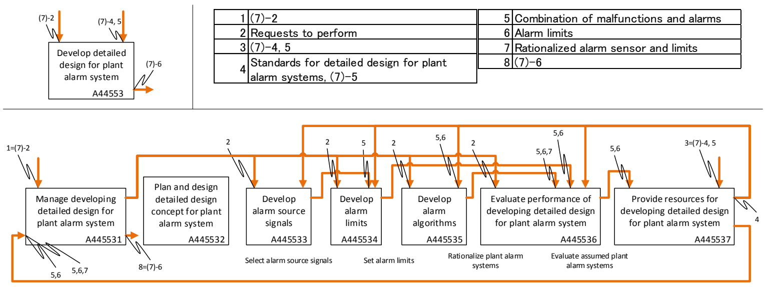
1) Perform cause-effect analysis for assumed malfunctions,
2) Select alarm source signals,
3) Set alarm limits,
4) Evaluate assumed plant alarm systems,
5) Rationalize plant alarm systems.

The characteristic nodes A44533 and A44563 are illustrated in **Figure 5**. It is assumed that the other nodes are following the above mentioned BPM. In the node A44533 in Figure 5 (1), the activity A445334 performs cause-effect analysis for assumed malfunctions.

In the node A44563 in Figure 5 (2), the activity A445633 selects alarm source signals, the activity A445634 sets alarm limits. In accordance with the evaluation results of the design in the activity A445636, the activity A445435 rationalizes plant alarm systems. The design procedures of the Luo method could be traced on the proposed BPM. The proposed BPM could be validated. Furthermore, it is confirmed which activities generate information using the plant alarm system design process.



(1) A44533 (Perform PHA) node



(2) A44563 (Develop detailed design for plant alarm system) node

Fig. 5 A part of business flow of Luo method

Conclusion

In the present paper, we tried to express a BPM concerned with a plant alarm system. Even if the developed BPM is incomplete, the BPM approach has following merits.

1. Design rationale for the plant alarm system can be specified and stored.
2. The plant alarm system can be designed more logically.

The stored design rationale and the logically designed plant alarm system are very useful for management of the change of the plant alarm system and ensuring consistency with other safety instruments.

Acknowledgment

This research has been conducted under the Japan

Society of the Promotion of Science (JSPS) 143rd committee on Process Systems Engineering.

Literature Cited

Center for Chemical Process Safety (CCPS), Layer of Protection Analysis – Simplified Process Risk Assessment, pp.75－113, John Wiley and Sons, Hoboken, U.S.A. (2001)

Fuchino, T., Y. Shimada, T. Kitajima and Y. Naka; "Management of Engineering Standards for Plant Maintenance based on Business Process Model," *Proceedings of 20th European Symposium on Computer Aided Process Engineering*, pp.1363－1368, Ischia, Italy (2010)

Instrumentation, Systems, and Automation Society (ISA); Management of Alarm Systems for the Process Industries, North Carolina, U.S.A. (2009)

Luo, Y., X. Liu, M. Noda and H. Nishitani; "Systematic Design Approach for Plant Alarm Systems," *J. of Chem. Eng. of Japan*, **40(9)**, pp.765－772 (2007)

National Institute of Standards and Technology (NIST); Integration Definition for Function Modelling (IDEF0), Federal Information Processing Standards Publication, 183, *National Institution of Standards and Technology* (1993)

PIEBASE (Process Industry Executive for Achieving Business Advantage using Standards for Data Exchange) Activity Model Executive Summary (1998)

Shimada, Y., T. Kitajima, T. Fuchino and K. Takeda; "Disaster Management Based on Business Process Model Through the Plant Lifecycle, Approaches to Managing Disaster - Assessing Hazards, Emergencies and Disaster Impacts," *InTech*, 19－40 (2012)