Incident Investigation on the basis of Business Process Model of Plant Lifecycle Engineering Activities for Process Safety Leading Metrics

Tetsuo Fuchino[a], Kazuhiro Takeda[b], and Yukiyasu Shimada[c]
[a] Chemical Engineering Dept., Tokyo Institute of Technology, Tokyo, Japan
[b] Applied Chemistry and Biochemical Engineering, Shimizu University, Hamamatsu, Japan
[c] Chemical Safety Research Gr., National Institute of Occupational Safety and Health, Tokyo, Japan

Abstract: The process safety incidents are directly caused by defects of protection layers, and process safety management (PSM) system maintains the soundness of the protection layers. In general, it is said that the weakness in PSM system is identified from the incident cases, and the performance of the PSM is improve by PDCA cycle using process safety metrics. However, PSM business process is comprehended in the plant lifecycle engineering business process, so that even if the weakness of PSM system is identified, the key engineering business process for the weakness and metrics cannot be recognized, so far. To overcome the above mentioned problem on process safety metrics, we propose a business process model based process safety incident investigation for process safety metrics.

Keywords: Process Safety Management, Process Safety Metrics, Business Process Model, Incident Investgation, .

1. INTRODUCTION

The process safety incidents are directly caused by defects of protection layers, and process safety management (PSM) [1] system maintains the soundness of the protection layers. Process safety metrics [2] is intended to improve the performance of PSM system by Plan-Do-Check-Act (PDCA) cycle. The process safety metrics is categorized broadly into two types; lagging metrics and leading metrics. The lagging metrics is a retrospective set of metrics that are based on incidents. Events that occurred in an incident by passing through gaps in PSM system or protection layer can be described as lagging indicators. The leading metrics is a forward looking set of metrics which indicate the performance of the key business processes, operating discipline, or layers of protection that prevent incidents. In measuring lagging metrics, weakness in PSM system is identified, and the leading indicators which represent performance of the identified PSM system are to be selected for improving the performance by PDCA cycle. However, PSM business process is comprehended in the plant lifecycle engineering business process, so that even if the weakness of PSM system is identified, the key engineering business process for the weakness and leading metrics cannot be recognized, so far.

The authors have developed a business process model for plant lifecycle engineering (LCE) ([3], [4], [5]) as IDEF0 (Integration Definition for Function) activity model [6]. A plant lifecycle is composed of several engineering stages; process and plant design, plant construction, operation and plant maintenance. To make the consistent IDEF0 activity model ('To-Be' model), a novel template approach across all principal activities is used. For the process design engineering stage, independent protection layer (IPL) design concept [7] is applied, and performing process hazard analysis (PHA) and operational design are repeated. For the operation engineering stage, production plan and schedule are gradually detailed, and the pre-start review activity is defined before startup in operation explicitly. For the plant maintenance engineering stage, restoring is defined as the function of plant maintenance, and the risk based maintenance environment is modeled. The developed LCE business process model meets the requirements as the process safety management framework.

To overcome the above mentioned problem on process safety metrics, we propose a business process model based process safety incident investigation for process safety metrics. From the concept of IPL, a process safety incident would occur when events passed through gaps in protection system. Conversely, the incident could not happen if such a gap of the protection layer was removed. In this

study, root cause for remaining such a gap of protection layer is to be analyzed by tracing back over LCE business process model from the activity of relating protection layer, for a process safety incident. To illustrate the effective of the proposed approach, an explosion incident case, which is supposed from the incident occurred on March 23 in 2005 at BP Texas City Refinery Complex ([8], [9], [10]), is applied.

2. BUSINESS PROCESS MODEL FOR LCE

In this study, the PSM incident is investigated on the basis of a generic business process model. To make the generic model, a novel template approach across all principal activities was used. This template configures five types of activities, i.e. “Manage”, “Plan”, “Do”, “Evaluate”, and “Provide Resources”. The first four types represent the action, plan, do, check of PDCA cycle respectively, and the last one is to prepare information, resources and engineering standards. In this template as shown in **Figure 1**, “Manage” activity receives ‘Directives’ and ‘Output’ from the hierarchically upper parent activity, and outputs sub-‘Directives’ to “Plan”, “Do” and “Evaluate”. These activities are activated according to the sub-‘Directives’, and output ‘Certified Output’ to these locating on their downstream. The ‘Certified Outputs’ received by “Provide Resources” are furthermore informed to “Manage” as ‘Information for Management’. “Manage” approves the results of “Plan”, “Do” and “Evaluate”, and outputs ‘Certified Output’ to the parent activity. The “Provide Resources” receives ‘Engineering Standards’, ‘Resources’ and ‘Information’, and deliver them to “Manage”, “Plan”, “Do” and “Evaluate”. In case of trouble in “Plan”, “Do” and “Evaluate” activities, they output ‘Change Request’ or ‘Requirement for Provide Resources’ to “Manage” via “Provide Resources” as ‘Information for Management’. “Manage” may decide to inform these requirements to the parent activity.

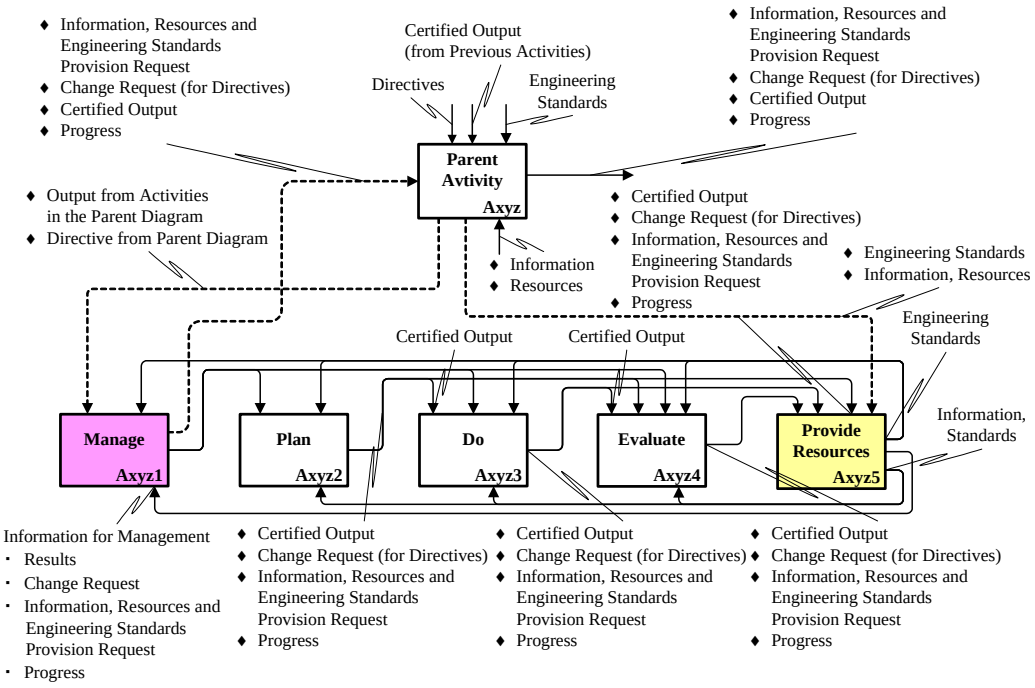

Figure 1 Template for Generalized Business Process Model

On the basis of the template, a business process model for plant lifecycle was provided. **Figure 2** shows a part of the model. In the template shown in Figure 1, the activity class of “Evaluate” is categorized, however this class of activity is omitted in the representation of plant lifecycle engineering activity model, here and after. The plant lifecycle engineering is composed of three engineering stages, i.e. plant and process design, construction, and production. Therefore, “A0: Perform LCE” is developed into six sub-activities, i.e. “A1: Manage LCE”, “A2: Plan Performing LCE”, “A3: Perform Process and Plant Design”, “A4: Construct Plant”, “A5: Perform Production”,

and “A7: Provide Resources for Performing LCE” by omitting A5 activity. Performing production is defined as production execution and maintaining the plant, so that “A5: Perform Production” is developed into “A51: Manage Production”, “A52: Make Production Plan”, “A53: Execute Production”. “A54: Perform Maintenance”, and “A56: Provide Resources for Production and Maintenance”. On the other hand, the process and plant are designed by conceptual, preliminary and final stages, and “A3: Perform Process and Plant Design” activity is developed into “A31: Manage Performing Process and Plant Design”, “A32: Plan and Design Overall Operational Design Philosophy”, “A33: Develop Conceptual Process Design (IPL-1)”, “A34: Develop Preliminary Process Design (IPL-2_7)”, “A35: Develop Preliminary Plant Design”, “A36: Develop Final Process Design”, “A37: Develop Final Plant Design” and “A39: Provide Resources for Performing Process and Plant Design”. In Figure 2, the box with the shadow expresses an activity to be developed into sub-activities, and the box painted over expresses an activity to be furthermore developed. In this study, “A34: Develop Preliminary Process Design (IPL-2_7)”, “A53: Execute Production” and “A54: Maintain Plant” activities are furthermore developed into children diagrams, and are utilized in the PSM incident investigation in the later section.

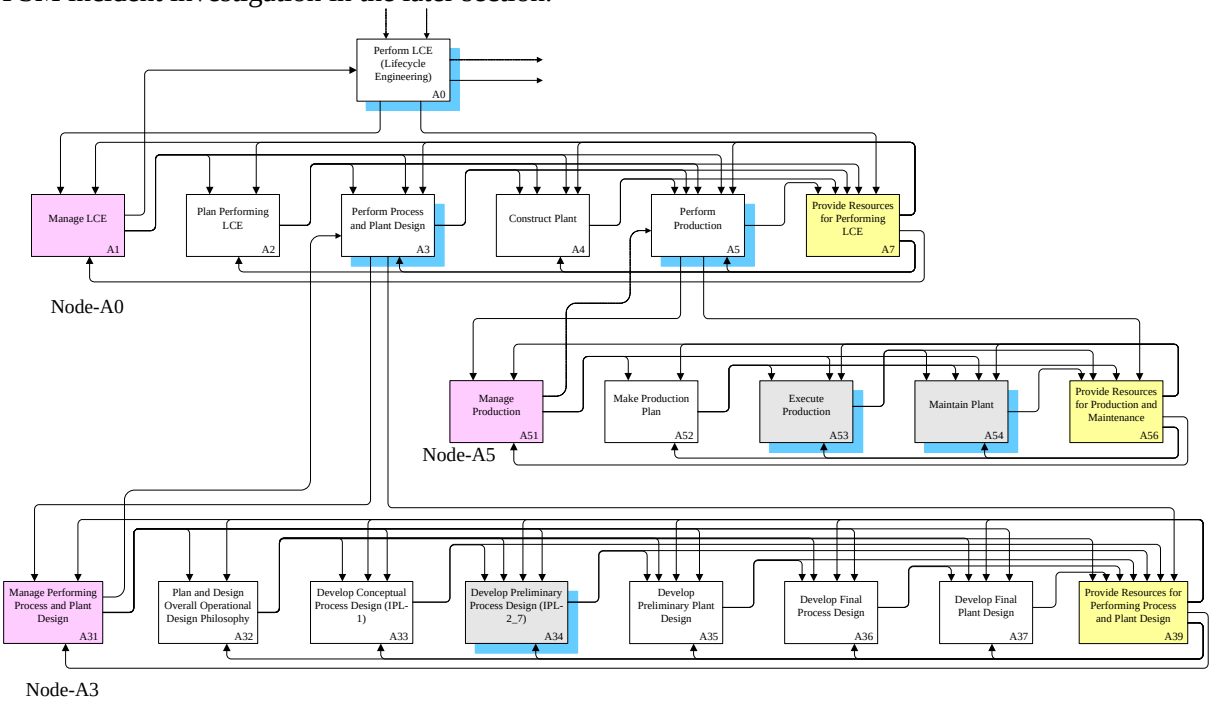

Figure 2 A Part of Business Process Model for Performing LCE

3. INCIDENT CASE

The incident during the startup operation of Raffinate Stripper Unit to separate C5/C6 components from non-aromatic raw material is supposed. The PFD of the Raffinate Stripper Unit is as shown in **Figure 3.** The outline of the sequence of events leading up to the incident is as following.

(1) Night shift operator overcharged Raffinate Splitter. LI (Level Indicator) indicated incorrect level due to the overcharge. LA (Level Alarm) of Raffinate Stripper had been out of order, and alarm was gone.
(2) Day shift operator began startup operation without noticing overcharge; starting circulation of furnace, starting charging and lighting furnace, without opening LCV (Level Control Valve) against operating procedure.
(3) Level, pressure and temperature of Raffinate Stripper were increased.
(4) Pressure of Raffinate Stripper was released by 8B RV (Relief Valve) bypass valve against operation manual.
(5) The operator opened the LCV by noticing closeness of the LVC. Raffinate Stripper inlet temperature was increased.

(6) Boiled oil overflowed, and RVs were opened. The boiling oil was fed to Blow Down Drum, and the drum was filled with boiling oil. From the open stack of the Blow Down Drum boiling oil was released to the air. Vapor cloud was formatted, and explosion was occurred.

From the view point of protection layer concept, if the protection layers performed properly, the incident should have been prevented. However, because of the following defects of the protection layers, the abnormal events led to the incident.

(a) Inappropriate type of instrumentation (LI).
(b) Incomplete maintenance (LA).
(c) Lack of engineering standard for restart up condition in case of unidentifiable abnormal situation.
(d) Lack of engineering standard for shutdown condition in case of fatal operation procedural error.
(e) Disconnection of RVs outlet Blow Down Drum to the flare line.

These defects of protection layers are considered as the direct causes for propagating the abnormal events to the incident. However, the root causes of these direct causes should be analyzed to consider the chemical safety leading metrics, and applying the LCE business process model for this analysis is proposed. We have analyzed the root causes for the direct causes of above (b), (d) and (e). The root cause analysis for only (e) is explained in the next section.

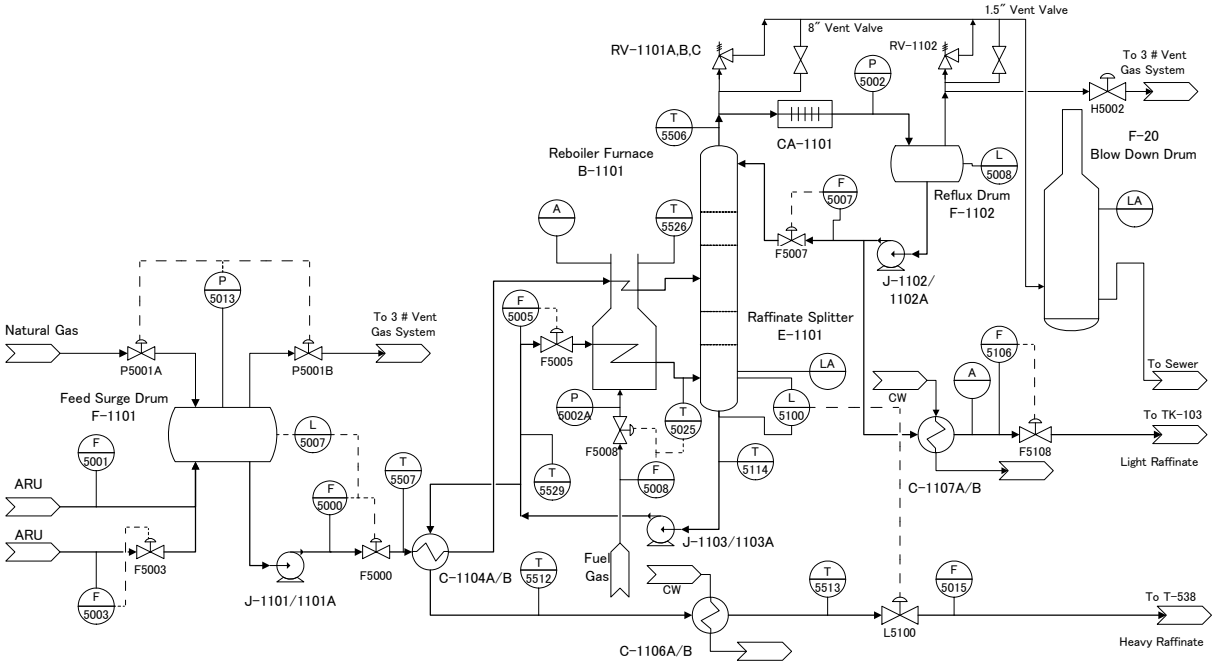

Figure 3 Process Flow Diagram of Raffinate Stripper Unit

4. INCIDENT INVESTIGATION ON LCE BUSINESS PROCESS MODEL

In any incident cases, the sequence of events leading up to the incident was clarified, and then the defects of protection layers and activity corresponding to the protection layers would be identified. Therefore, the analysis of root causes for a direct cause can be started from such an identified activity. For this failed activity, there must exist an unsafe condition (information) to make the protection layer failed, and another activity to output such an unsafe condition (information). The tracing back from the direct cause of incident to the root causes can be carried out by reputation of identifying a failed activity and unsafe condition. The unsafe condition can be categorized into four; i.e., unsafe condition for operation, unsafe condition for design, unsafe condition for maintenance and unsafe condition for decision making, and are described in red, purple, orange and blue lines respectively, here and after.

4.1. Trace Back Analysis for Production Related Root Causes

By using the incident case mentioned above, the root cause analysis from the defect of protection layer where Blow Down Drum did not connected to the flare line is carried out. In this incident case, even

though the Raffinate Stripper was overflew with boiling oil, RVs were operated and Blow Down Drum was filled with boiling oil, the incident would not occur, if the stack of the Blow Down Drum had been connected to the flare line. This defect of protection layer was revealed as releasing boiling oil to atmosphere in the emergency operation. Therefore, the investigation is started from "A534432: Execute Emergency Operation" activity, as shown in **Figure 4-1**. The fault of "A534432" is caused by providing 'the plant, whose Blow Down Drum stack is not connected to the flare line (Red 1)', and this unsafe condition is provided by the "A534434: Provide Resources for Emergency Operation".

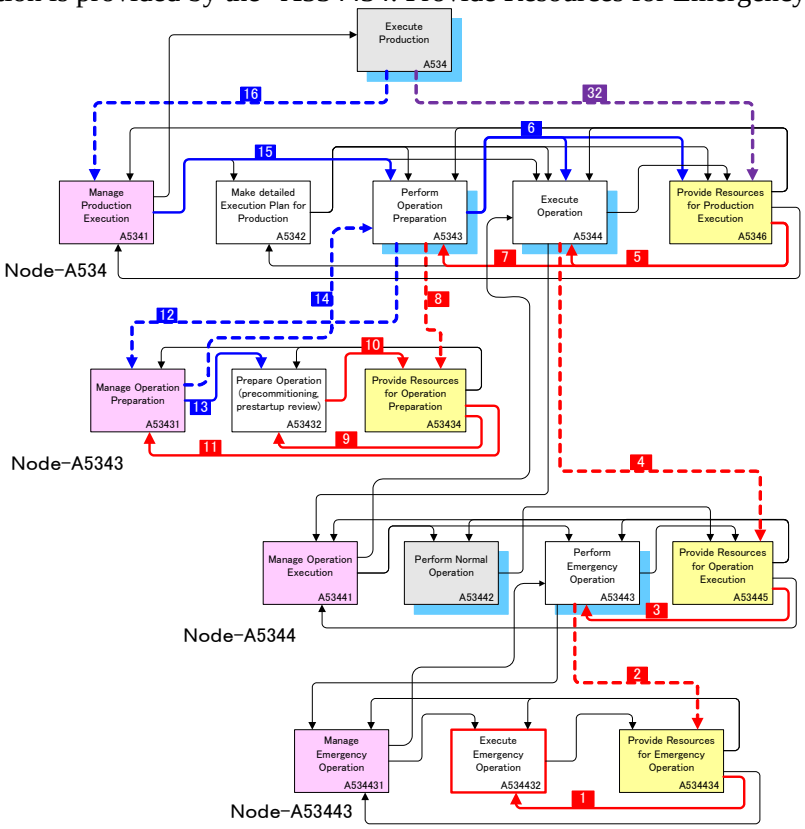

Figure 4-1 Root Cause Analysis on LCE Business Process Model (1)

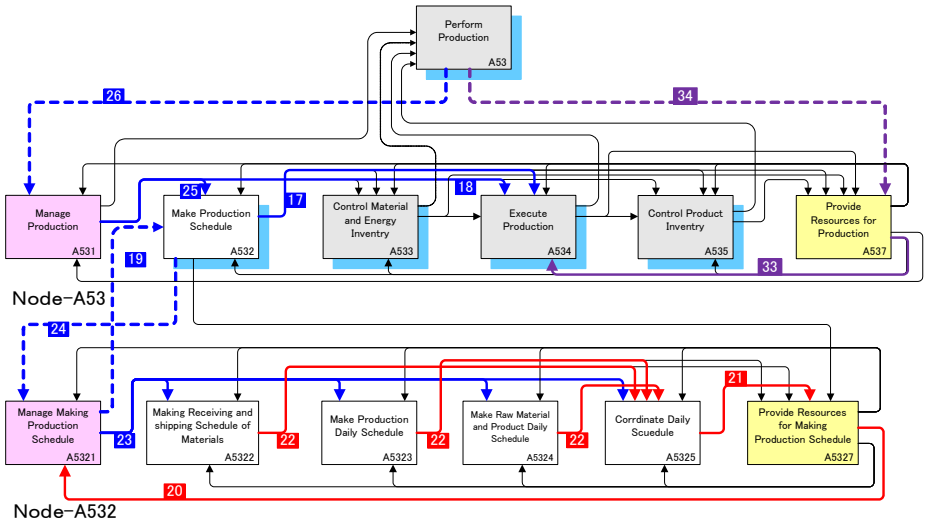

Figure 4-2 Root Cause Analysis on LCE Business Process Model (2)

In the same manner, tracing back the unsafe condition and activity generating the unsafe condition is repeated (Red 1 to 11) as shown in Figure 4-1. It is found that "A53431: Manage Operation

Preparation" activity certified use of the plant, whose Blow Down Drum stack is not connected to the flare line. The "A53431" activity, which is "Manage" class activity painted over with pink and converts the production related unsafe condition (Red 11) into the decision making (or safety culture) related unsafe condition (information) (Blue 12,13,14), becomes one of the key gates for starting up such an unsafe plant, whose Blow Down Drum stack is not connected to the flare line. Therefore, this certification should be one of the root causes.

The certification is carried out on the basis of the directive (Blue 12) as shown in Figure 4-1 of 'priority of cost and production'. This directive is furthermore traced back until "A534: Execute Production" (Blue 12 to 16) in Figure 4-1. This policy consists with that of "A532: Make Production Schedule" provided in "A5321: Manage Making Production Schedule" in **Figure 4-2.** As same as the "A53431" activity, "A5321" is "Manage" class activity painted over with pink, converts the production related unsafe condition (Red 20) is converted into the decision making (or safety culture) related unsafe condition (information) (Blue 19,23,24), and this activity is also one of the key gates for certifying the production policy of 'priority of cost and production'. Therefore, this certification should be the other root causes.

The overall production policy of "cost conscious" (Blue 26) in Figure 4-2 should be decided by the hierarchically upper decision making level. The production policy is further traced back from "A53: Execute Production" to "A0: Perform LCE (Lifecycle Engineering)" as shown in **Figure 4-3**, and the policy of "priority to cost and production" should have been decided as the Lifecycle Engineering policy (Blue 31).

Tables 1(1) and **1(2)** are the list of the unsafe information in the trace back analysis for production related root causes.

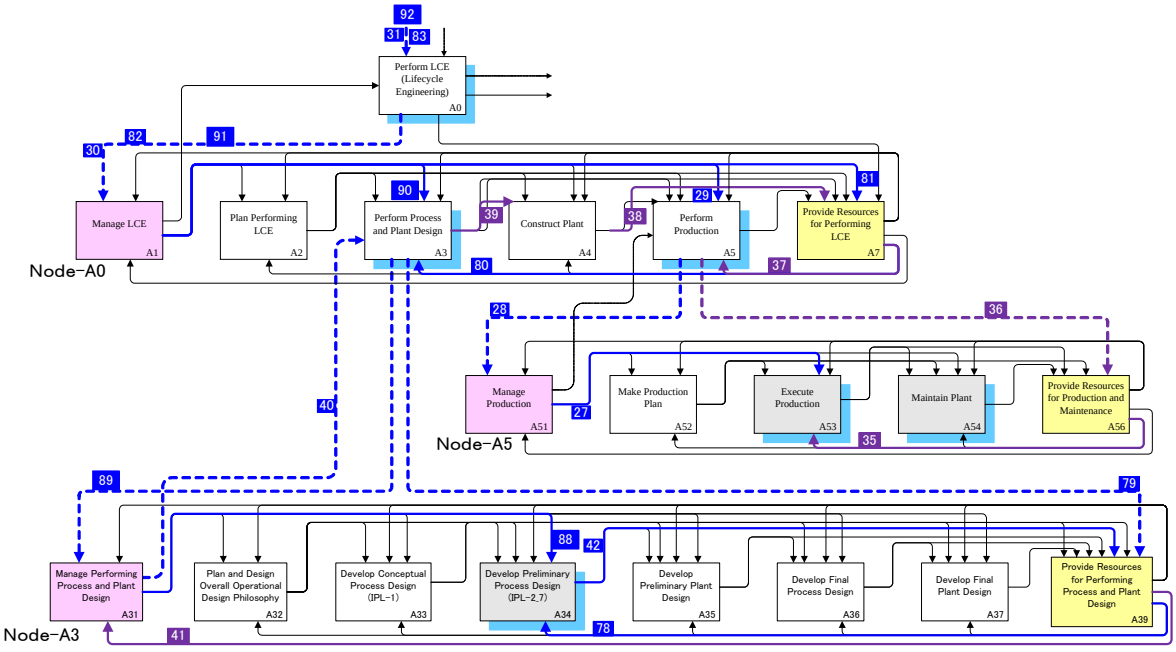

Figure 4-3 Root Cause Analysis on LCE Business Process Model (3)

Table 1(1) List of Unsafe Information for Operation Related Activities

Traced Infor.	Unsafe Information
1	The plant, whose Blow Down Drum stack is not connected to the flare line.
2	
3	
4	
5	
6	Approval of start-up the plant, whose blow down drum is not connected to plare line.

Table 1(2) (Continued)

7 8 9	The plant, whose Blow Down Drum stack is not connected to the flare line.
10 11	Plant change request to connect vent stack of the blow down drum to the flare line.
12 13	Start-up policy to start up the plant without connecting the stack of blow down drum to the flare line for the priority of cost and production.
14 15	Approval of start-up the plant, whose blow down drum is not connected to flare line for the priority of cost and production.
16	Production execution policy to continue production by the plant without connecting the stack of blow down drum to the flare line for the priority of cost and production.
17	Production execution plan, gaving priority to the early restart-up being conscious of cost.
18	Directive to make production execution plan, gaving priority to the early restart-up being conscious of cost.
19	Production execution plan, gaving priority to the early restart-up being conscious of cost.
20 21 22	Production execution plan for starting up the plant without conecting the stack of the blow down drum to the flare line.
23	Directive to make production execution plan for starting up the plant without conecting the stack of the blow
24 25 26	Directive to make production execution plan, gaving priority to the early restart-up being conscious of cost.
27 28 29 30	Directive to make production execution plan giving the priority to cost and production.
31	Directive to perform LCE giving the priority to cost and production.

4.2. Trace Back Analysis for Design Related Root Causes

After the production related root cause analysis, design related root causes are considered. As same in the previous section, “A5346: Provide Resources for Production Execution” activity is traced back form “A534432: Execute Emergency Operation” activity via unsafe information (Red 1 to Red 5) as shown in Figure 4-1. The plant, whose blow down drum is not connected to flare stack line, is designed in “A3: Perform Process and Plant Design” and informed it to “A5346” activity, via “A4”, “A7”, “A5”, “A56”, “A53”, “A537” and “A534” activities and unsafe information (Purple 39 to 32) as shown Figures 4-1 to 4-3. “A3” activity is developed into “A31” to “A37”, and the process safety design is performed in “A34: Develop Preliminary Process Design (IPL-2_7)” activity as shown in Figure 4-3. The process design around RV and Brown Down drum is performed in “A345: Develop Preliminary Process Design for Abnormal Situation” activity as shown in **Figure 4-4**, and the “process structure, whose blow down drum is not connected to flare stack line” information (Purple 48) is output from “A3455: Develop Design for Total Shutdown” activity as shown in **Figure 4-5**. Such a process structure without connecting blow down drum to the flare stack line is selected at “Node-A34553” shown in **Figure 4-6,** based on the scope of process design for emergency total shut down operation (Purple 59), which is limited to RVs activation. This scope is decided on “Node-A34552”, and certified at “A34551: Manage Design for Total Shutdown” activity on the basis of the directive information (Blue 67) to design process with open RV system. This directive is caused by insufficient result (Purple 71 shown in Figure 4-5), that the stripper over overfilling and bumping are not considered for RV activation cause and result, output from “A34522: Perform PHA for Preliminary Process Design for Abnormal Situations” activity. “A34522” was performed on the basis of insufficient information on past experienced trouble and incident (Blue 7 to 83), and unsuitable PHA execution directive that operation after RV activation is not included (Blue 84 to 92)as shown in Figures 4-5, 4-4, 4-3.

Table 2 shows the list of the unsafe information in the trace back analysis for production related root causes. As mentioned in section 4.1, the design related root causes are the activities of “Manage” categorized ones that changing the information lines colored by purple to blue. Therefore, the defects of “A345521: Manage Preliminary Operations for Partial Shutdown”, “A3451: Manage Preliminary

Process Design for Abnormal Situations" and "A1: Manage LCE" are found to be the design related root causes.

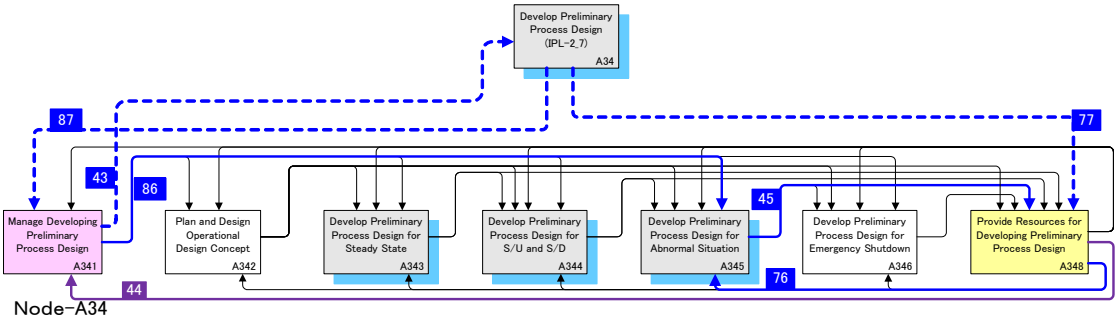

Figure 4-4 Root Cause Analysis on LCE Business Process Model (4)

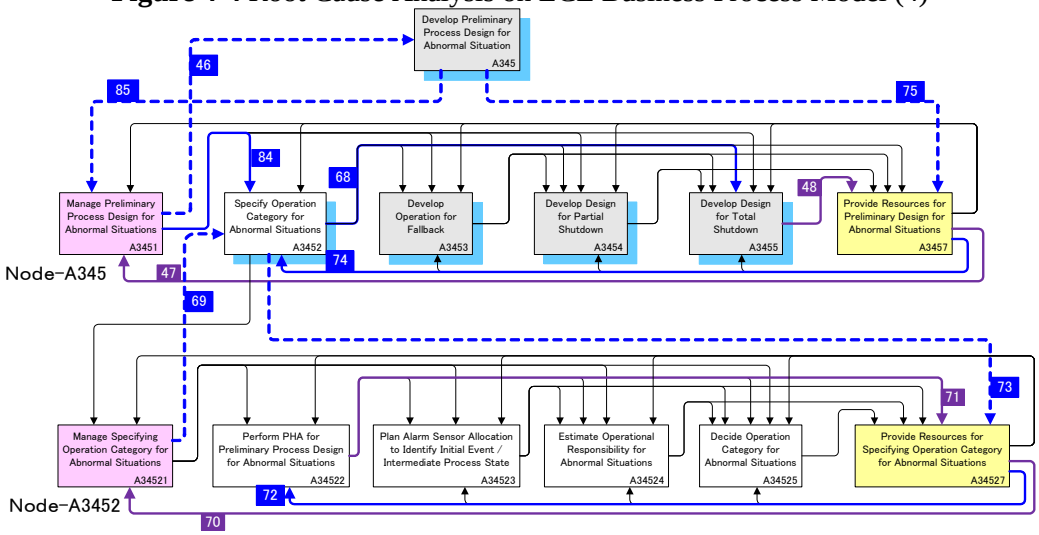

Figure 4-5 Root Cause Analysis on LCE Business Process Model (5)

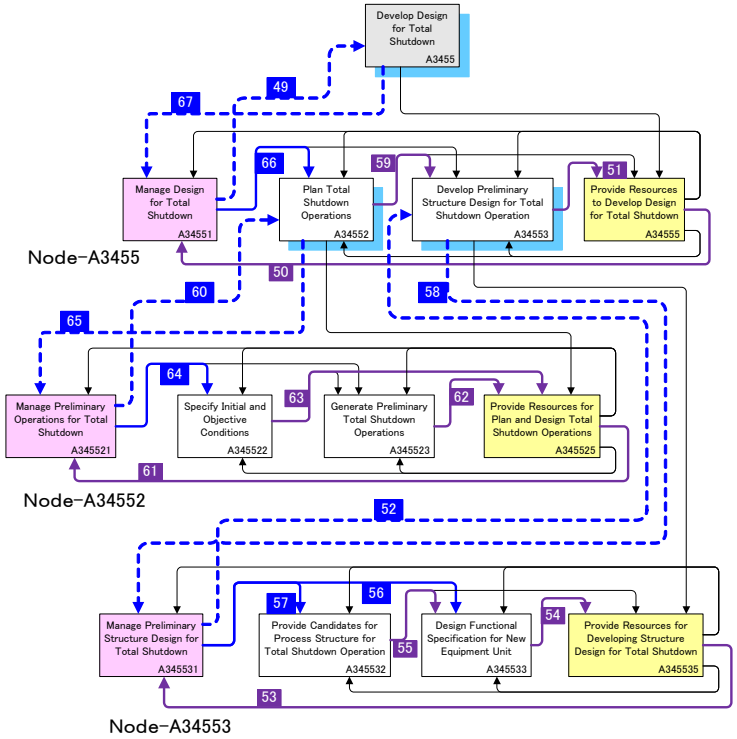

Figure 4-6 Root Cause Analysis on LCE Business Process Model (6)

Table 2 List of Unsafe Information for Design Related Activities

Traced Infor.	Unsafe Information
32	The plant, whose blow down drum is not connected to flare stack line.
33	
34	
35	
36	
37	
38	
39	The process, whose blow down drum is not connected to flare stack line
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	
51	Process structure, whose blow down drum is not connected to flare stack line
52	
53	
54	
55	Process structural alternative, whose blow down drum is not connected to flare stack line
56	Directive to select process structural alternative, whose blow down drum is not connected to flare stack line
57	Directive to include the process structure, whose whose blow down drum is not connected to flare stack line,
58	Specification of the initial and target emergency shutdown operating conditions for process structural design
59	Scope of process design for emergency total shut down operation; until RV activated.
60	
61	
62	
63	
64	Directive of operational design for emergency total shut down to specify scope of process design; until RV activated.
65	
66	
67	
68	Stripper overfilling and bumping are not included in RV activation cause and result. Insufficient PHA for after RV activated.
69	
70	
71	
72	Insufficient information on past experienced trouble and incident. Stripper overfilling and bumping is not included
73	
74	
75	
76	
77	
78	
79	
80	
81	
82	
83	
84	Unsuitable PHA execution directive. Operation after RV activation is not included.
85	
86	
87	
88	
89	
90	
91	
92	

4. CONCLUSION

Process safety metrics is intended to improve the performance of PSM system by Plan-Do-Check-Act (PDCA) cycle. The process safety metrics is categorized broadly into two types; lagging metrics and leading metrics. The lagging metrics is a retrospective set of metrics that are based on incidents. Events that occurred in an incident by passing through gaps in PSM system or protection layer can be described as lagging indicators. The leading metrics is a forward looking set of metrics which indicate the performance of the key business processes, operating discipline, or layers of protection that prevent incidents. In measuring lagging metrics, weakness in PSM system is identified, and the leading indicators which represent performance of the identified PSM system are to be selected for improving the performance by PDCA cycle. However, PSM business process is comprehended in the plant lifecycle engineering business process, so that even if the weakness of PSM system is identified, the key engineering business process for the weakness and leading metrics cannot be recognized, so far. To overcome this problem, we propose a business process model based process safety incident investigation for process safety metrics. From the concept of IPL, a process safety incident would occur when events passed through gaps in protection system. Conversely, the incident could not happen if such a gap of the protection layer was removed. In this study, root cause for remaining such a gap of protection layer is to be analyzed by tracing back over LCE business process model from the activity of relating protection layer, for a process safety incident.

References

[1] Occupational Safety and health Administration, “Process Safety Management,” OSHA 3132, (2000).

[2] Center for Chemical Process Safety “Guidelines for Process Safety Metrics”, Wiley, (2010).

[3] Fuchino, T., Y. Shimada, T. Kitajima and Y. Nakad, "Management of Engineering Standards for Plant Maintenance based on Business Process Model," Computer-Aided Chemical Engineering, 28, PP 1363-1368, (2010).

[4] Shimada, Y., M. Kumasaki, T. Kitajima, K. Takeda, T. Fuchino and Y. Naka, "Reference Model for Safety Conscious Production Management in Chemical Processes," Proceedings of 13th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, PP 629-632, (2010).

[5] Fuchino, T. Y. Shimada, T. Kitajima, K. Takeda, R. Batrese and Y. Nakaf, "Business Process Model for Process Design being that Incorporates Conscious of Independent Protection Layer Considerations", Computer-Aided Chemical Engineering , 29, PP 362- 330, (2011).

[6] IST, "Integration Definition for Function Modelling,” Federal Information Processing Standards Publication, 183, http://www.itl.nist.gov/fipspubs/idef02.doc, National Institution of Standards and Technology. (1993).

[7] Drake, E. M., "An Integrated Approach for Determining Appropriate Integrity Levels for Chemical Process Safety Interlock Systems," Proceedings of Int. Symposium and Workshop on Process Safety Automation, Houston, PP 225-248 (1994).

[8] US Chemical Safety Board, " FATAL ACCIDENT INVESTIGATION REPORT, Isomerization Unit Explosion Final Report Texas City, Texas, USA", //www.csb.org/ (2005).