CHEMICAL ENGINEERING TRANSACTIONS
VOL. 48, 2016
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Eddy de Rademaeker, Peter Schmelzer

ISBN 978-88-95608-39-6; **ISSN** 2283-9216
DOI: 10.3303/CET1648149

Incident Investigation on the Basis of Business Process Model for Plant Lifecycle Engineering

Tetsuo Fuchino*[a], Kazuhiro Takeda[b], Yukiyasu Shimada[c]

[a] Tokyo Institute of Technology, 2-12-1, O-okayama, Meguro-ku, Tokyo 152-8552, Japan
[b] Shizuoka University, 3-5-1, Johoku, Naka-ku, Hamamatsu 432-8011, Japan
[c] National Institute of Occupational Safety and Health, Japan, 1-4-6, Umezono, Kiyose, Tokyo, 204-0024, Japan
fuchino@chemeng.titech.ac.jp

The process safety incidents are directly caused by defects of protection layers, and process safety management (PSM) system should maintain the soundness of the protection layers. In general, the weakness of the PSM system is identified through the incident investigations, and the performance of the PSM has to be improved through the PDCA cycle using process safety metrics. However, PSM business process is comprehended in the plant lifecycle engineering business processes, so that even if the weakness of PSM system is identified, the key engineering business processes for that weakness cannot be recognized, so far. To overcome the above mentioned problem on process safety metrics, we propose the business process model based process safety incident investigation for process safety metrics.

1. Introduction

The process safety incident investigations play important roles for process safety management (PSM), not only to develop corrective measures for these process safety incidents, but also to improve the performance of PSM system through Plan-Do-Check-Act (PDCA) cycle. In these days, for the purpose of the improvement of the PSM performance, the process safety metrics (AIChE/CCPS, 2010) came to attract attention. The process safety metrics is categorized broadly into two types; lagging metrics and leading metrics. The lagging metrics is to identify the weaknesses of the PSM system from the incident investigations, and the leading metrics is to improve the performance of the PSM business processes of which weaknesses were recognized. It is desirable to generate the leading metrics on the basis of the identified weaknesses of the PSM by the lagging 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 processes for the weaknesses and leading metrics cannot be recognized, so far.
The authors have developed a business process model for plant lifecycle engineering (LCE) (Fuchino et al., 2010, 2011; Shimada et al., 2010) as IDEF0 (Integration Definition for Function) activity model (NIST, 1993). 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 (Drake, 1994) 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-up review activity is defined before start-up 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 modelled. 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 incident investigation approach to generate leading metrics. From the concept of IPL, a process safety incident would occur when events passed through gaps in the protection system. Conversely, the incident could not occur if such gaps in the protection layer had been removed by the PSM in the lifecycle engineering business process. The sequence of the critical events leading to an incident can be found by the event tree

Please cite this article as: Fuchino T., Takeda K., Shimada Y., 2016, Incident investigation on the basis of business process model for plant lifecycle engineering, Chemical Engineering Transactions, 48, 889-894 DOI:10.3303/CET1648149

analysis technique. These events can be considered as the contribution causes for the incident, and the more process safety managerial causes for the respective critical event are analysed by tracing back over the LCE business process model from the activities where the critical events occurred (Fuchino et al., 2015). In this study, on the basis of the results of the proposed analysis approach, the activities whose errors became the root causes for the respective contribution causes are identified. From the identified activities, the defects of the process safety management can be found, and the leading metrics to measure the performance of the process safety management can be obtained. To illustrate the effectiveness of the proposing incident investigation approach, an explosion incident case, which is supposed from the incident occurred on March 23, 2005 at the BP Texas City Refinery Complex (US Chemical Safety Board, 2005), is applied.

2. Template and LCE business process model

In this study, the PSM incident is analysed 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 “act”, “plan”, “do” and “check” of PDCA cycle respectively, and the last one is to prepare information, resources and engineering standards. The ICOM (Input, Control, Output and Mechanism) of each type of activities in the template includes these classes of information shown in Figure1 to configure the PDCA (Plan, Do, Check and Act) cycle within and across the hierarchical activity nodes.

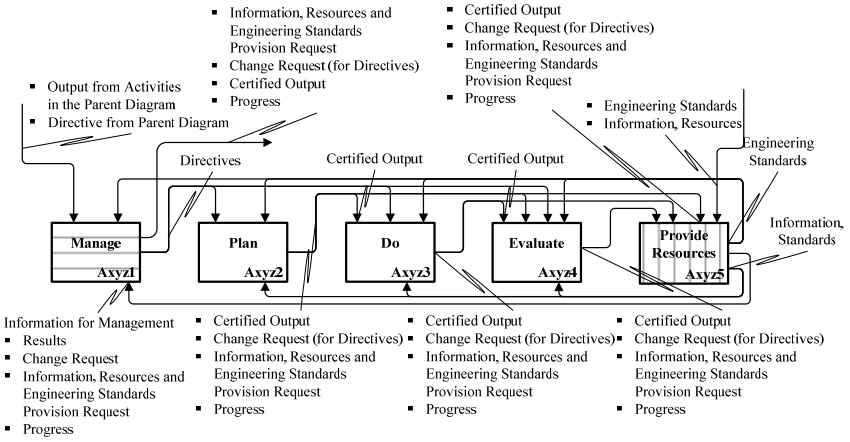

Figure 1: Template for the generic business process model.

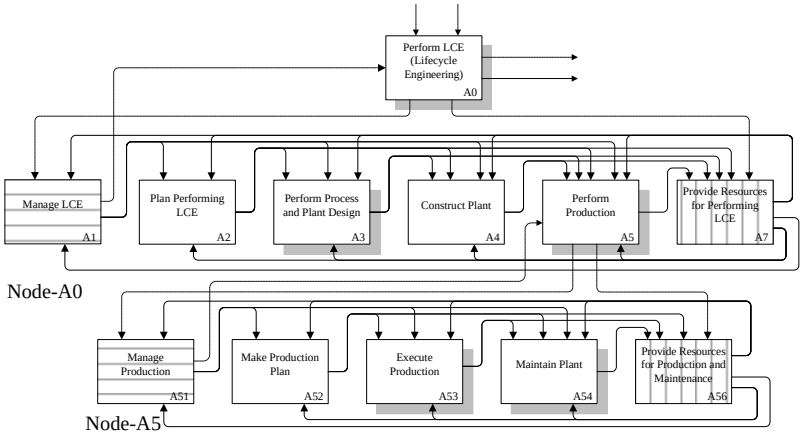

Figure 2: A part of LCE business process model.

On the basis of the template, a business process model for performing plant lifecycle engineering had been developed. 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. The “Performing Production” activity is

defined as production execution and maintaining the plant. In Figure 2, the shadowed boxes express activities to be developed into sub-activities, and the hatched boxes with horizontal lines express “Manage” activities, and these with vertical lines express “Provide Resources” activities.

3. Incident investigation

3.1 Incident case

In this study, the incident during the start-up operation of the raffinate stripper unit is supposed. In this unit, the non-aromatic raw material from the aromatics recovery unit (ARU) is separated at C5/C6 cut point into the light and heavy raffinates. The incident began in the overcharge of raw materials and, after some critical operational failure, the raffinate stripper was filled with boiled oil, and the overhead relief valves (RVs) were opened. The boiling oil was fed into the blow down drum, and the drum was filled with boiling oil. Because, the stack of the blow down drum was not connected to the flare line, the boiling oil was released to the air. The vapour cloud was formed, and the vapour cloud explosion occurred.

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

(a) Inappropriate type of instrumentation of the level indicator.
(b) Incomplete maintenance of the level alarm.
(c) Lack of engineering standard for restart up condition in case of abnormal situation.
(d) Lack of engineering standard for shutdown condition in case of fatal operation procedural error.
(e) Disconnection of the RVs outlet blow down drum to the flare line.

These defects in protection layers are considered as the contribution causes of this incident. To consider the chemical safety leading metrics, the root causes of these contribution causes should be analysed by applying the LCE business process model. The root cause analysis for the last contribution cause (e) is explained here.

3.2 Tracing back over the LCE business process model

The tracing back over the LCE business process model from the activity where the above critical event due to the defect of the protection layer on the relief valve outlet line is performed here. This critical event occurred at “A534432: Execute Emergency Operation” activity because the emergency operation was performed in the plant that the outlet of the blow down drum did not connected to the flare line. The tracing back is carried out along the ICOM (Input, Control, Output and Mechanism) information involving such unsafe conditions. The unsafe conditions 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 with black bold solid lines, black bold broken lines, black bold dotted lines and gray bold solid lines respectively. It is obvious that the root causes from a contribution cause should be the decision-making error, so that we paid attention to the “Manage” categorized activities where the type of the representation of the unsafe condition is changed to the gray bold solid one. Furthermore, the errors of activities are concerned, there are two types of errors in activities can be considered on the basis of the tracing back from the “A534432” activity, one is errors on the activities of operation as shown in Figures 3 and 4, and the other is errors on the activities of the design as shown in Figure 5.

Figure 3 shows the tracing back from the “A534432” activity, which is marked with the circle of the broken line to “A534” activity, and the decision-making of “A53431: Manage Operation Preparation” activity which approved the start-up operation of the plant of which the blow down drum outlet line did not connect to the flare line is found to be one of the root causes. In Figure 4, the same tracing back operation as shown Figure 3 is proceeded from the “A534: Execute Production” activity to “A0: Perform LCE” activity. The decision-making of “A53431: Manage Making Production Schedule” activity which directed to make production execution plan for starting up the plant without connecting the stack of the blow down drum to the flare line, and approved the cost conscious production execution schedule that made much of early production start is found to be the other root cause. Furthermore, the decision-making of “A1: Manage LCE” activity which directed to make production execution plan giving the priority to cost and production is found to be the root cause.

On the other hand, Figure 5 traced back the PSM errors on the activities of the design from the “A534432” activity. The process and plant without connecting the stack of the blow down drum to the flare line was provided from “A7: Provide Resources for Performing LCE” activity, so that the tracing back is started from “A7” activity along the ICOM information involving unsafe conditions. The “A34521: Manage Specifying Operation Category for Abnormal Situations”, “A3451: Manage Preliminary Process Design for Abnormal Situations” and “A1: Manage LCE” activities are found to be the “Manage” categorized activities which made errors in decision-making. “A34521” activity approved the insufficient PHA for RVs activation, and “A3451” activity directed insufficient PHA execution directives. “A1” activity did not promote enhancement of the PHA activity or active use of the experienced incident information to predict process safety incidents.

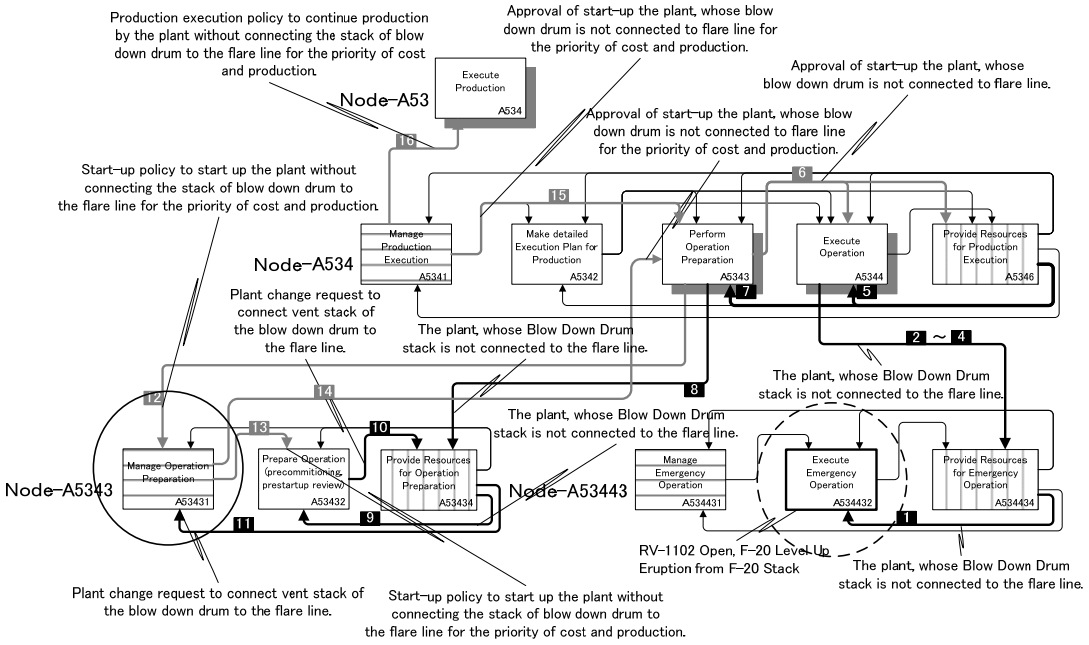

Figure 3: Tracing back over the LCE business process model from "A534432" to "A534" activities to find the defects of the activities of operation.

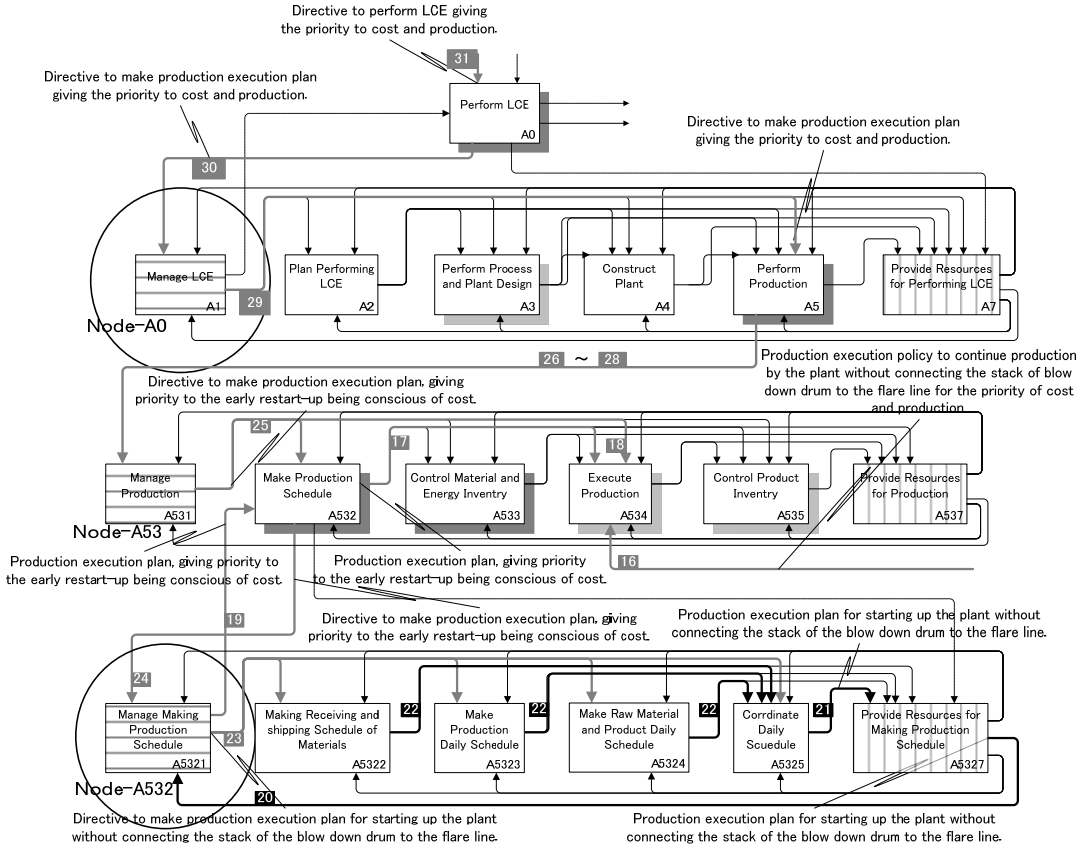

Figure 4: Tracing back over the LCE business process model from "A534" to "A0" activities to find the defects of the activities of operation.

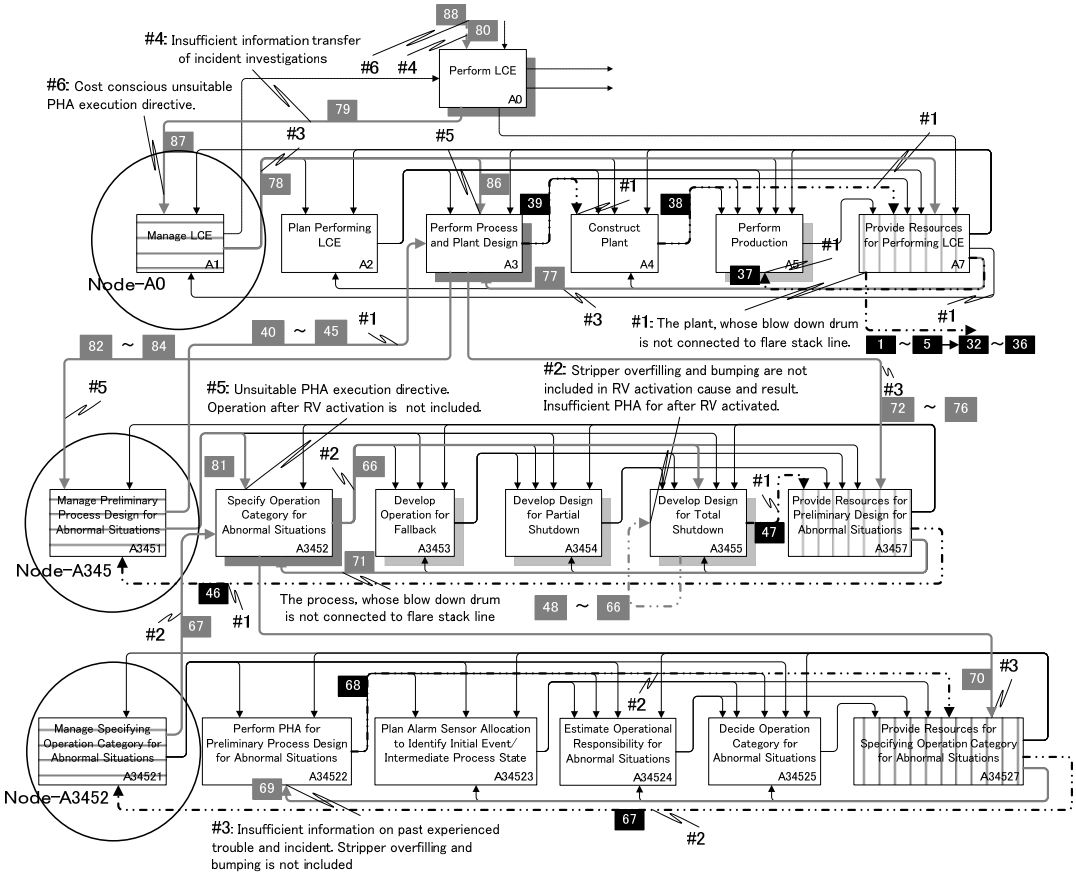

Figure 5: Tracing back over the LCE business process model from the "A7" activity to find the defects of the activities of process design.

3.3 Leading Indicator Generation

In this study, on the basis of the proposed analysis approach, the root causes for the respective contribution causes are found as the decision-making errors of the "Manage" categorized activities as shown with circle of solid line in Figures 3, 4 and 5. Furthermore, the proposed tracing back on the LCE business process model is carried out along the ICOM (Input, Control, Output and Mechanism) information involving the unsafe conditions. Therefore, the activities whose errors became the root causes for the contribution cause and the unsafe conditions of the ICOM information for the activities are identified. The element of process safety management corresponding to the identified business process can be revealed as shown in Table 1.

Table 1: Summary of Incident Investigation for Figure 3

ID	Activity Name	ICOM	Unsafe Information	Subject PSM
A53431	Manage Operation Preparation	M	Plant change request to connect vent stack of the blow down drum to the flare line.	Pre-start-up Safety Review
		C	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.	
		O	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.	
		O	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.	

The leading indicators to evaluate the performance of these activities can be considered on the basis of the input and output information as shown in Table 2. However, the performance of the pre-startup safety review and the process safety culture cannot be evaluate simply from the input and output information, so that the referring to the published guidelines is recommended in Table2.

Table 2: Candidates of Leading Indicators

ID	Leading Indicator Candidates
A53431	Guidelines for Auditing Process Safety Management Systems：Operational Readiness
A5321	(Number of Process/Plant Structural Change Completed before Start-up) // (Number of Process/Plant Structural Change Required)
A1	Guidelines for Auditing Process Safety Management Systems：Process Safety Culture (1) General PSM Culture Issues, (2) BP Texas City Investigation Cultural Indicator
A34521	(Number of Operating Conditions after RVs and SIS Activated on which PHA is Performed) // (Number of Hazard Scenarios to Activate RVs and SIS) (Number of Inciden / Trouble Cases Investigated in PHA) // (Number of Inciden / Trouble Cases Occured in Past)
A1	Guidelines for Auditing Process Safety Management Systems：Process Safety Culture (1) General PSM Culture Issues, (2) RBPS Cultural Indicators
A3451	(Number of Operating Cases of RVs/SIS Activation that Environmental Impact is Investigated) // (Number of Operating Cases of RVs/SIS Activation)
A1	Guidelines for Auditing Process Safety Management Systems：Hazard Identification and Risk Analysis

4. Conclusion

To improve PSM performance through the plant lifecycle using PDCA cycle, the process safety metrics plays an important role, and the proper leading metrics should be identified from the fatal and/or near miss incidents. In this study, a business process model of performing lifecycle engineering based incident investigation is proposed. On the basis of the LCE business process model, tracing back over the model is performed and the activities whose errors became the root causes for the respective contribution causes are identified. From the identified activities, the defects of the process safety management can be found, and the leading metrics to measure the performance of the process safety management can be obtained.

Reference

Center for Chemical Process Safety (AIChE/CCPS); “Guidelines for Process Safety Metrics,” Wiley, (2010)

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, 225-248, Houston, U.S.A. (1994)

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

Fuchino, T., K. Takeda, Y. Shimada and A. Aoyama, “Business Process Model Based Incident Investigation for Process Safety Leading Metrics”, 48, 8, 626-633, J. of Chem. Eng. of Japan (2015)

National Institute of Standards and Technology (NIST), "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)

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, 629-632, Brugge, Belgium (2010)

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