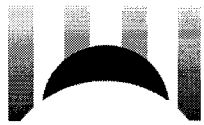

5th Annual Symposium, Mary Kay O'Connor Process Safety Center
"Beyond Regulatory Compliance: Making Safety Second Nature"
Reed Arena, Texas A&M University, College Station, Texas
October 29-30, 2002

A Framework for Designing Independent Protection Layer (IPL) Implementing Process Hazard Analysis to Process Safety Design

Hiroshi Sumida*, Atsushi Aoyama, Yoshio Kawauchi, Tetsuo Fuchino, Rafael Batres, Yukiyasu Shimada, Kazuhiro Takeda, Nobuo Takagi, Yuji Naka
*System Safety and Reliability, Applied Technology Section, R&D Center,
Toyo Engineering Corporation, Japan
2-8-1, Akanehama, Narashino-shi, Chiba 275-0024, Japan
E-Mail: sumida-hiroshi@ga.toyo-eng.co.jp
Phone: +81 47 454 1937

ABSTRACT

Despite the clarity of Process Safety Design concept, the current safety design seems to be done using heuristics and experiences of process designers and safety engineers. Because of this, the quality of safety design is heavily dependent on the expertise of those engineers.

The proposed framework expresses the process as a design of independent protection layer (IPL). A scenario-based approach is introduced to support the design of ILP 3, 4 and 5 utilizing design rationales. The key parameters are integrated in the framework, such as Risk (Severity, Frequency), Propagation Speed of hazard, Propagation Paths, Affected area, and sensors to support making rational decisions.

The proposed framework is found effective for supporting "Process Safety Information" and "Management of Change" required by US OSHA-PSM.

INTRODUCTION

The "Process Safety Design" concept seems to have been well established according to various codes, standards, regulations, design practices and guidelines.

However, the more concerns are:

- The current safety design approach may allow ad-hoc design implementation that would result in lack of explicit design rationale. This may cause unbalanced safety design, forcing unnecessary provisions or leading to negligence of safety precaution.

- The mechanism is not explicitly defined to make rational decision on protection layers.

Safety as one of the major characteristic of a plant is determined as a function of process design (process physicochemical behavior), plant design (or hardware configuration), and control & operational design (or operational management).

While considering an abnormal situation, the resultant would be recovery, partial shutdown, or total shutdown. Classifying the operation category following abnormal situation into these three operation modes, verification may become easier as partial shutdown, or total shutdown will be furnished with common provisions and some exceptions, irrespective of the initiating event of abnormal situation.

While considering a precaution for an abnormal situation, the major concern would be if we have ample time and sufficient number of appropriate sensors so that we can detect appropriated process deviation in time and cope with the particular abnormal situation.

Apparently, another view is risk-based approach. While applying this approach, the key parameters are Severity of consequence, Frequency of occurrence, and propagation speed of hazard. The propagation speed is converted into the available time to cope with the abnormal situation while considering the mitigation.

Design Rationales and appropriate tools are another important factors as foundation of decision making and judgement.

With the above background hold, this paper focuses:

- Express the activities of "Process Safety Design" with design rationales, identifying the relationships among the concerned information.
- The activity model will be structured a scenario-based which will be categorized recovery, partial shutdown, or total shutdown.

INDEPENDENT PROTECTION LAYER

The Independent Protection Layer (IPL) [1, 2] concept has been commonly used to distinguish the safety measures. Table 1 presents the classification of safety layers and functional requirements of the IPL by interpretation.

Table 1: Independent Protection Layer (IPL)

IPL	Classification	Functional Requirement
1	Process Design	Reduce Risk by implementing inherently safer process design.
2	Basic Controls, Process Alarms, and Operator Supervision	Control the fluctuation of operating parameter within the normal operating range.

IPL	Classification	Functional Requirement
3	Critical Alarms, Operator Supervision, and Manual Intervention	When operating parameter deviates for some reason and approaches to the critical limit of normal operational range, a critical alarm will draw operator's attention and require intervention. There must be sufficient time available for operator's judgement and response.
4	Automatic Action SIS or ESD	When operating parameter deviates widely from the normal operational range in a short period of time approaching to the tolerable limit, automated safety instrumented system (emergency shutdown) shall respond to prevent the system from relieving the materials contained to the atmosphere.
5	Physical Protection (Relief Device)	Irrespective of inner protection layers, there is a potential of overpressure due to not only internal reason but also external reason such as external fire. Pressure relief valve is a last resort.
6	Physical Protection (Dikes)	Should the containment be failed, the hazardous materials released to atmosphere should be localized to minimize the external impact.
7	Plant Emergency Response	Plant wide Emergency Response Organization with necessary provisions such as gas detectors, emergency communication system, fire brigade, etc.
8	Community Emergency Response	Community wide Emergency Response Organization with necessary provisions

These IPLs should be evaluated scenario by scenario for all the identified potential hazard scenario in order to ensure the integrity of a protection layer or a combination of protection layers.

Despite the IPLs, a hazard may propagate and breakthrough over the IPLs depending on the failure of each IPL. Figure 1 shows such potential variances of the process parameter indicating different path of breakthrough over the IPLs, Operation limit in terms of product quality, Mechanical Design limit in terms of containment integrity, and IPL.

The IPL2 is of more concern on product quality. Most of the plant lifecycle, the IPL2 would be the major player.

The IPL3, IPL4 and IPL5 are to be solely provided for the mitigation of hazards in order to maintain the containment integrity. Therefore, from the viewpoint of incident prevention, the IPL3, 4, and 5 should have the important role for prevention and mitigation.

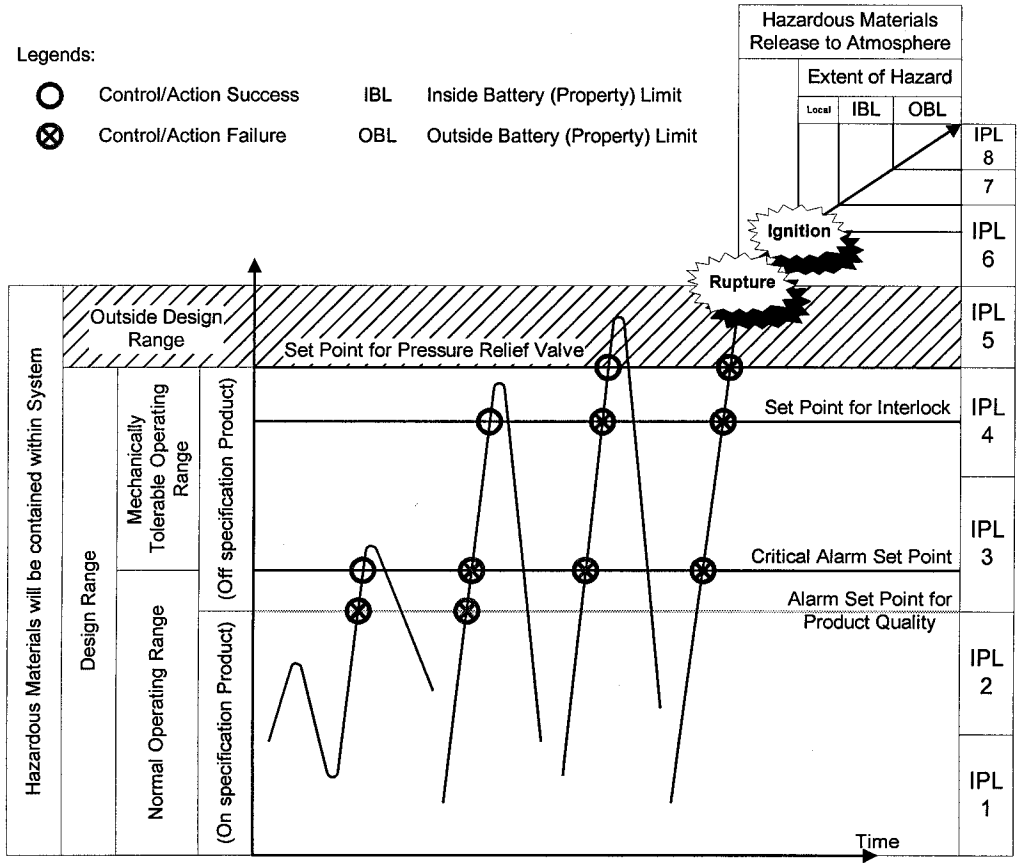

Figure 1: Potential Hazard Propagation over IPLs

The provision of IPL5, that is pressure relieving devices such as pressure relief valve or rupture disk will be primarily determined according to the code requirements and/or regulatory requirements.

However, there is a potential of providing SIS (IPL4) in lieu of IPL5 as follows.

According to API RP 521 [3] (Guide for Pressure Relieving and Depressuring Systems), 2.2 Overpressure Criteria, the following exception is given.

"In addition, some relieving scenarios require the installation of high-integrity protective instrument systems to prevent overpressure and/or over-temperature. If this approach is used, the protective instrument system shall be at least as reliable as a pressure-relief device system, and shall be used only when the use of pressure relief device is impractical."

ASME Case 2211 [4] accepts the Overpressure Protection by System in lieu of the Pressure Relief Device under particular condition.

In order to recognize the current practice of safety design corresponding to the IPL, the commonly applied safety measures and check lists for safety design were investigated, and categorized.

Figure 2 shows a mapping of the current practice of safety measures and concerns over the IPL. The arrow indicates the direction of information from one design consideration to the others.

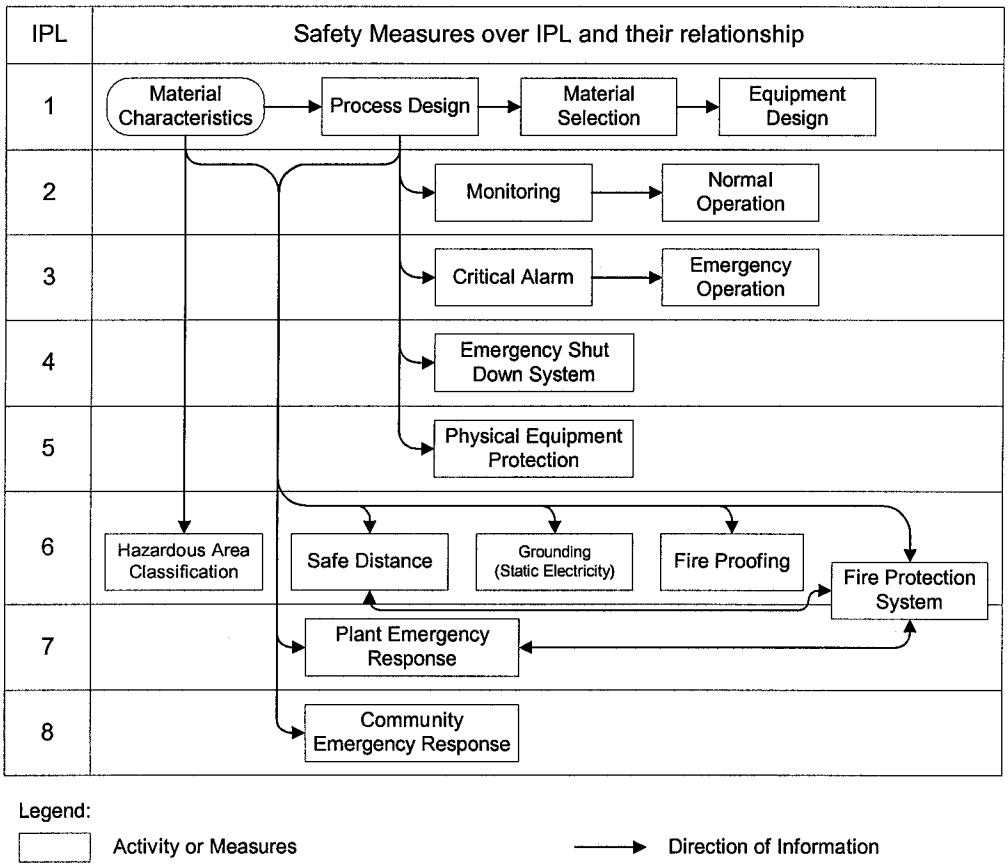

Figure 2: Safety Measures on each IPL and Relationships

Note that the other safety concerns such as Regulatory Requirements, Codes & Standards, Occupational Safety, Lightning Protection, Building Design are excluded from Figure 2.

Since IPL 6 usually refers to "Physical Protection", there may be an open question for mapping the "Hazardous Area Classification", "Safety Distance", "Grounding (Static Electricity)", "Fire Proofing", and "Fire Protection" to IPL 6. However, the authors considered those safety measures the IPL 6 category in this study, as they were provided for the protection in case of loss of containment.

As observed, the IPL2, 3, 4, and 5 are developed based on the information available in IPL1. Similarly, IPL6, 7, and 8 are usually developed based on the information available in IPL1 regardless of provisions of IPL2, 3, 4, and 5.

This fact may be interpreted that the IPL6, 7, and 8 tend to be determined based on the regulatory requirements, codes and standards, and there is a potential of release due to failure of inner IPLs. IPL7 and 8 may be influenced by the IPL2 to 6, or vice versa.

From the viewpoint of process safety design based on the scenario-based approach which is closely related with the process design and the importance of incident prevention, the authors determined to focus the study scope for the IPL3, 4, and 5.

SCENARIO-BASED PROCESS HAZARD ANALYSIS

Presentation Method of Model

IDEF0 was used as function modeling method to present the activity models of "A Framework of designing Independent Protection Layer (IPL)". Figure 3 shows the IDEF0 presentation.

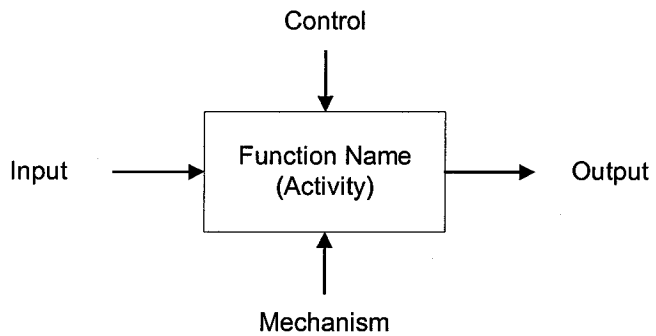

Figure 3: IDEF0 Presentation

Each side of the function box has a standard meaning in terms of box/arrow relationships. The arrow interfaces presents the arrow's role. Arrows entering the left side of the box are inputs. Inputs are transformed or consumed by the function to produce outputs. Arrows entering the box on the top are controls, which specify the conditions or constraint required for the function to produce correct outputs. Arrows leaving a box on the right side are outputs, which are the information/data or objects produced by the function. Arrows connected to the bottom side of the box represent mechanisms that support the execution of the function.

Activity Model of Process Hazard Analysis and Safety Design

Applying the IDEF0 methodology, the activity model was developed from the viewpoint of designing safety as shown on Figures 4 - 14. (These figures are located at the last part of this paper on the block.)

The scenario-based approach is primarily divided into two steps. The first step is a categorization of abnormal situation into recovery, partial shutdown, and total shutdown as a result of process hazard analysis. The second step is a designing IPLs for each category of abnormal situation.

Assuming that the IPL5 is primarily determined according to the code requirements and/or regulatory requirements, the IPL5 is not shown on the activity models. Rather, as mentioned earlier, the activity model for the IPL5 design in combination with IPL4 design may be required, for which authors had not developed.

Develop Conceptual Process Design for Abnormal Situation (A213)

It is assumed that the activities "Develop Conceptual Process Design for Steady State (A211)" and "Develop Conceptual Process Design for Startup (SU) and Shutdown (SD) (A212) have been completed.

Thus, the "Operational Flow Diagram (OFD) from SU and SD" was considered available as an input to the "Process Design for Abnormal Situation (IPL 3, 4, 5) (A213)". The management of mechanism (e.g. Design and Engineering Resources) and assessment criterion were assumed ready to use.

Figure 4 shows that the activity (A213) will use this OFD from SU and SD, and generate the following outputs under the controls listed below.

Outputs:

Functional Equipment Specifications, Preliminary Operating Procedures, Software Sensor Information, SIS Logic (Requirements), Time/Cost Estimation, Operational Flow Diagram (OFD) from Design for Abnormal Situations, Modification Request for Preliminary Plant Design

Controls:

Process Flow Diagram (PFD), Owner Requirements, Regulatory and Societal Requirements, Design Basis, Equipment Specifications and Equipment List, Plot Plan and Layout

The activity (A213) was further developed to manage different category of abnormal situations as shown in Figure 5. Under this activity, "Operation Category" is directed to the relevant function box of Recovery (Fallback) (A2132), Partial Shutdown (A2133), or Total Shutdown (A2134).

Manage Design for Abnormal Situation (A2131)

Figure 6 shows the activity of "Manage Design for Abnormal Situation".

Under the activity (A21311), "Initiating Event" which could result in potential hazard is generated based on OFD from SU and SD. The "Initiating Event" will be Equipment Failures, Material Failure at System Boundary (MFSB), or Mal-operation (Operator Error).

With the given initiating event and other process information, "Process Hazard Analysis" is carried out under the activity (A21312) to generate "Frequency of Initiating Event and probability of each propagation path", "Severity of each propagation path", "Affected area (propagation paths, areas and speed), and "Risk Level".

With the information on "Affected area (propagation paths, areas and speed), "Risk Level", and other process related information, operation category will be determined under the activity (A21313) to provide recommendation on monitoring point for process variable to detect cause and/or effect, and operation category.

Perform Process Hazard Analysis (PHA) (A21312)

Figure 7 shows the activity of "Perform Process Hazard Analysis (PHA)".

Under the activity (A21312), two levels of process hazard analysis by means of qualitative and/or quantitative will be carried out depending on the complexity of the hazard scenario.

With the information on Initiating Event, Material Safety Data Sheet (MSDS), Reliability Data, and other process information, qualitative process hazard analysis will be carried out under the activity (A213121) to generate Severity (Relative Ranking), and Information on Propagation paths and area.

In case the predetermined condition is met, such as high severity determined by the qualitative process hazard analysis or recommended by qualitative PHA, quantitative process hazard analysis will be carried out under the activity (A213122) to generate Severity, and Information on Propagation paths and area quantitatively.

In case process response is not obvious or there is no sufficient experience to estimate the process response margin, a dynamic simulation may be required (A213123) to evaluate if there is sufficient time for operator's intervention after process alarm for quality control is initiated.

Specify Operation Category (A21313)

Figure 8 shows the activity of "Specify Operation Category".

With the information on "Affected area (propagation paths, areas and speed)" and other process information, the process variable is evaluated if it is feasible to detect cause and/or effect as a result of initiating event in question. If detection is validated feasible, appropriate process variable and monitoring point are investigated and proposed.

If detection and suitable monitoring are validated feasible in time, with the information on "Risk Level", other process related information, and feedback from (A2132) and (A2133) if any, operation category will be determined under the activity (A213132).

Then, this determined "Operation Category" is discharged from the function box (A2131) on Figure 5 via the function box (A21313) on Figure 6, and then connected to the relevant function box of operation category Recovery (Fallback) (A2132), Partial Shutdown (A2133), or Total Shutdown (A2134).

Develop Design for Recovery (Fallback) (A2132)

Figure 9 to Figure 13 present the activities under the "Develop Design for Recovery (Fallback)". The similar activities will apply to the underneath hierarchy of the Partial Shutdown (A2133) and Total Shutdown (A2134), which are not included in this paper.

Figure 9 shows that the activity "Manage Operation for Fallback" (A21321) will generate relevant "Initiating Events". Then, the activity "Plan Operations and generate Flow sheet alternatives for Fallback" (A21322) can generate the "Operating Procedure for Single Initiating Event" and "Modified Process Flow sheet alternatives and Sensor location for single initiating event". Note that the information is to be generated as coordinated outputs from the activity (A21322).

The activity "Modify Plan Flow sheet for Fallback" (A21323) will then generate the "Process Flow sheet Information", "Hard Sensor Information", "Soft Sensor Information", and "Modified Operation Procedure for Fallback" which are fed back to the activity "Manage Operation for Fallback" (A21321).

Then, verification will be made based on the PHA Result (e.g. Frequency of Initiating Event and Probability of each Propagation Path, Severity of each Propagation Path, and Affected Area (Propagation Path, Areas, and Speed)).

Figure 10 shows that the aggregated initiating events are evaluated for simplification by the activity "Manage Operation for Fallback" (A21321).

Figures 11 and 12 show that Process Dynamic Simulation will be done under the activity "Determine Quantitative Operation Procedure" (A213221) to evaluate the feasibility of Fallback operation. If Fallback is judged feasible and sensor location is practicable, "Operation Procedure for Single Initiating Event (for Fallback)" and "Modified Process Flow sheet alternatives and Sensor location for single initiating event" are generated.
If Fallback is judged infeasible, scenario will be redirected to either Partial Shutdown (A2133), or Total Shutdown (A2134) by the activity "Manage Design for Abnormal Situation" (A2131).

Figure 13 and 14 show the optimizing process of process sensors.

Under the activity "Allocate Sensors for Detection of Cause and Fallback" (A213232), the sets of initiating events are sorted out according to the propagation speed. The sensors for high propagation speed are then integrated, and sensor(s) may be added for the low propagation speed. The sensor information is then fed back to the activity (A21321) for verification as mentioned above.

CONCLUSION

The proposed framework shows the decision making process with required information and resources explicitly, covering the safety operation management as well as the safety design of IPL3, 4, and 5.

The scenario-based approach is primarily divided into two steps.

At the first step, a categorization is carried out for abnormal situation into recovery, partial shutdown, and total shutdown as a result of process hazard analysis.

At the second step, the relevant IPLs are designed for each category of abnormal situation, according to the Risk (Severity, Frequency), Propagation Speed of hazard, Propagation Paths, Affected area, and sensors.

Collecting the information embedded in the activity models, the requirement of the Technology Infrastructure for supporting Process Safety Design will be established.

Using the proposed framework, the information registered in the course of designing IPLs and safety operation management becomes the process safety information showing the design rationales.

The proposed framework can be enhanced for supporting the Management of Change. Identifying the change in question as trigger point, trace the same path with the original design of the activity model until conflict may be found against the original design. Then, track the new path according to the change. This process leads to the final goal as a result of change. To do this, the information applied for the original design shall be maintained with appropriate identification.

As above, the proposed framework will support the two important elements of US Occupational Safety and Health Administration (OSHA) – Process Safety Management (PSM).

REFERENCE

[1] Guidelines for Engineering Design for Process Safety, American Institute of Chemical Engineers, Center for Chemical Process Safety, p.9, New York, NY, 1993

[2] Guidelines for Safe Automation of Chemical Processes, American Institute of Chemical Engineers, Center for Chemical Process Safety, pp.13-16, New York, NY, 1993

[3] American Petroleum Institute (API) Recommended Practice RP 521, Guide for Pressure-Relieving and Depressuring Systems, p.4

[4] American Society of Mechanical Engineers (ASME) Case 2211, 1996, Pressure Vessels with Overpressure Protection by System Design, Section VIII, Divisions 1 and 2

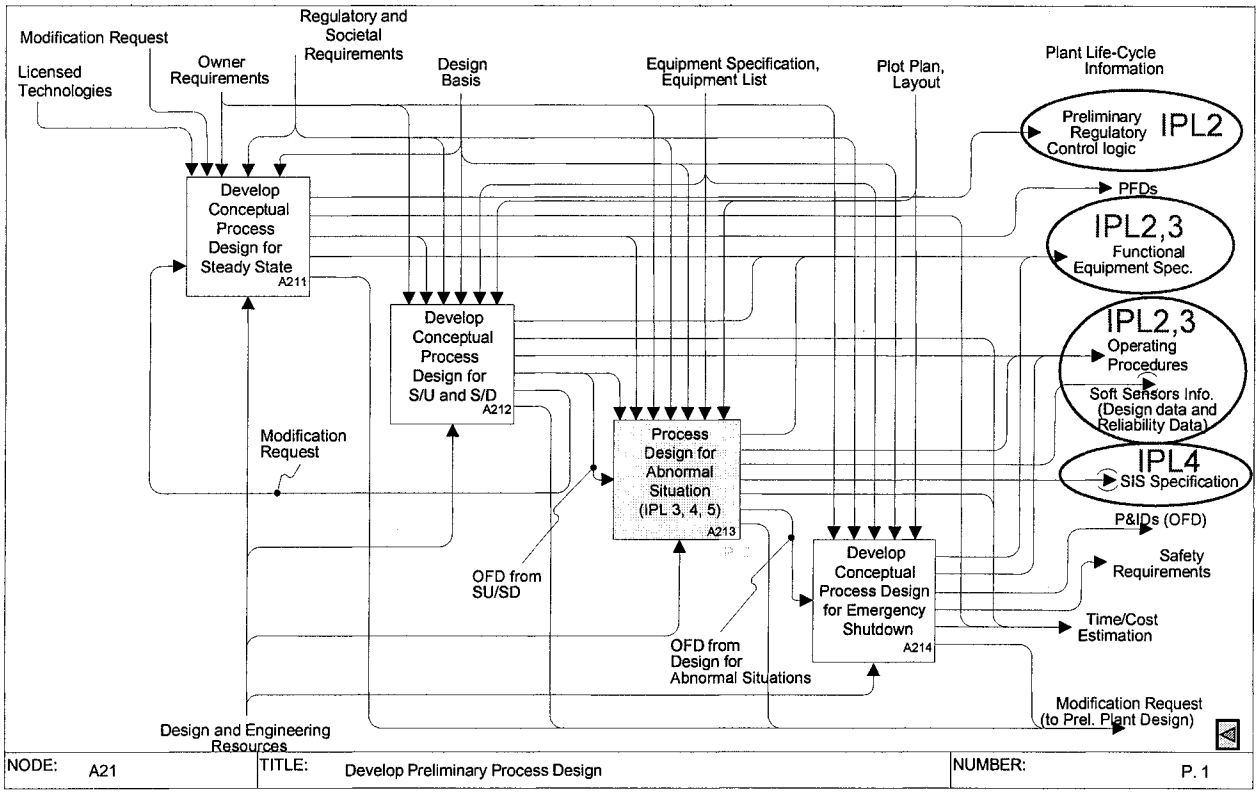

Figure 4: Activity Model – Develop Preliminary Process Design (A21)

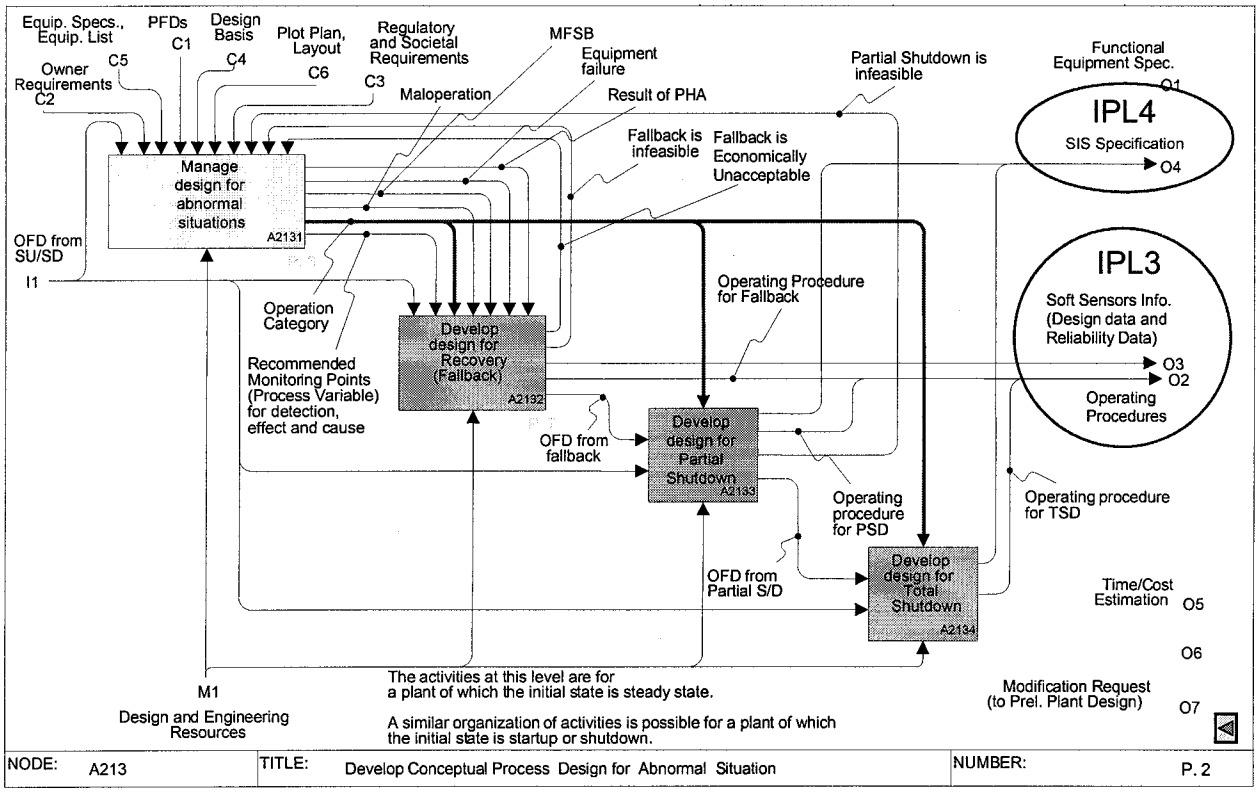

Figure 5: Activity Model – Develop Conceptual Process Design for Abnormal Situation (A213)

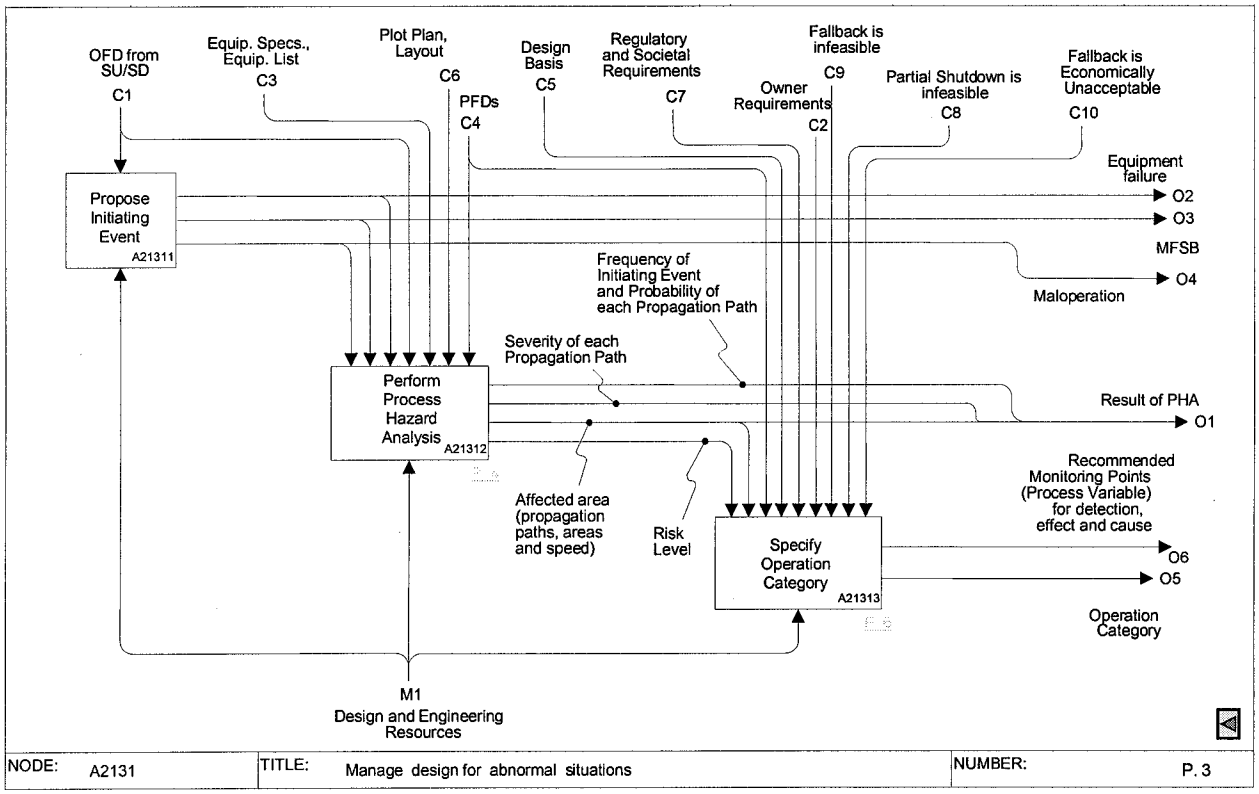

Figure 6: Activity Model – Manage Design for Abnormal Situations (A2131)

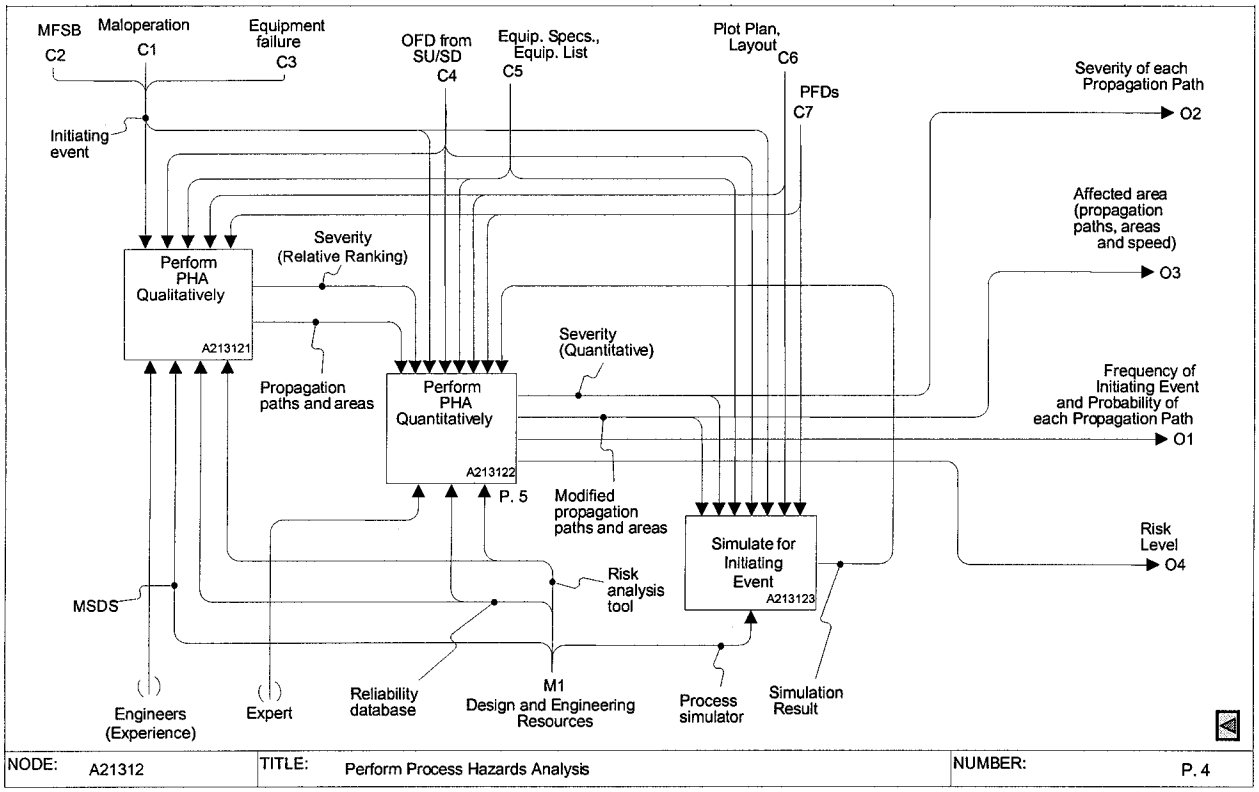

Figure 7: Activity Model – Perform Process Hazard Analysis (A21312)

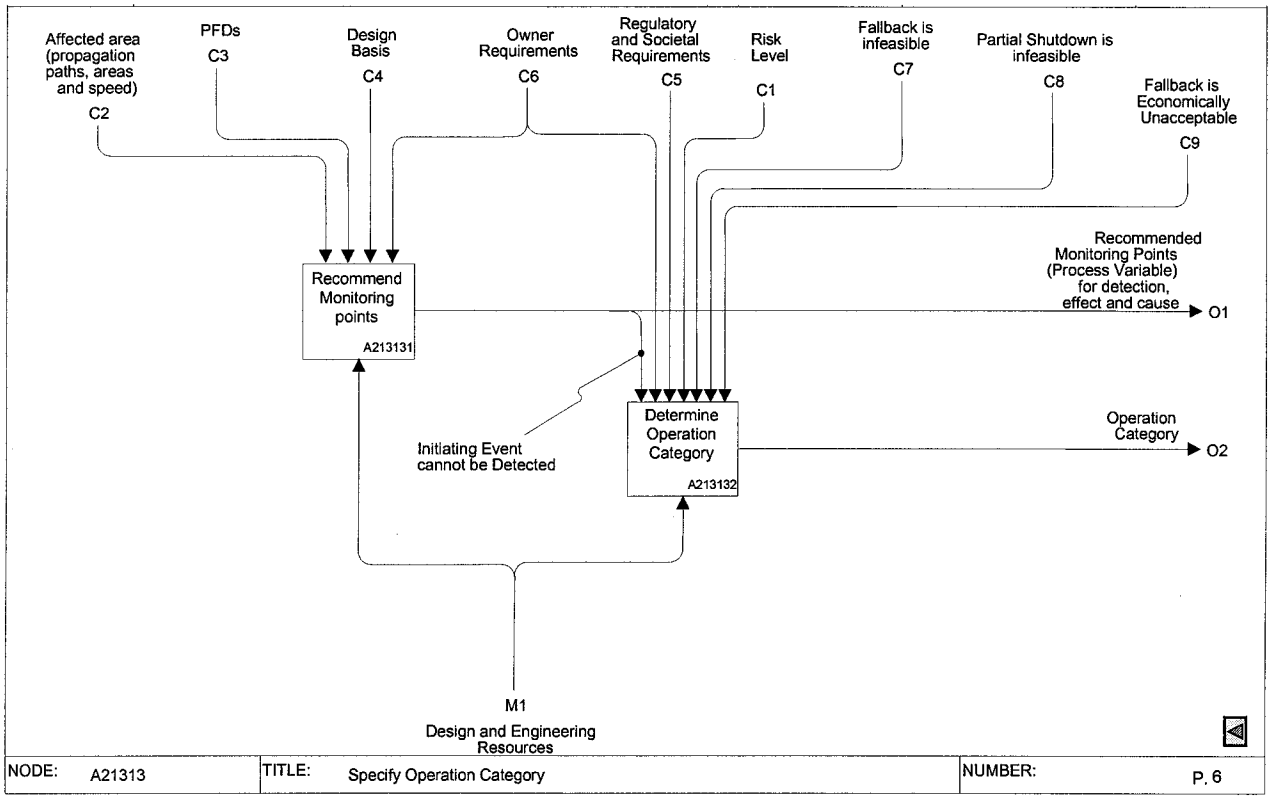

Figure 8: Activity Model – Specify Operation Category (A21313)

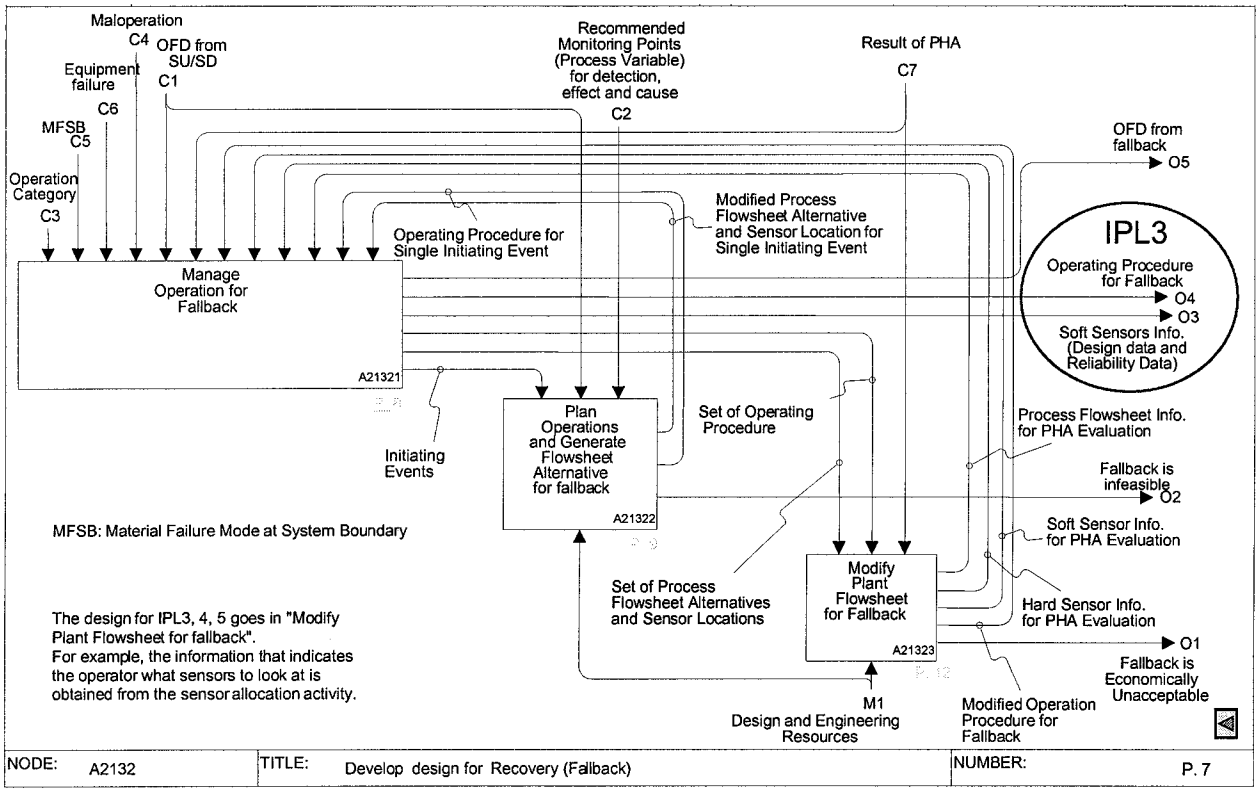

Figure 9: Activity Model – Develop Design for Recovery (Fallback) (A2132)

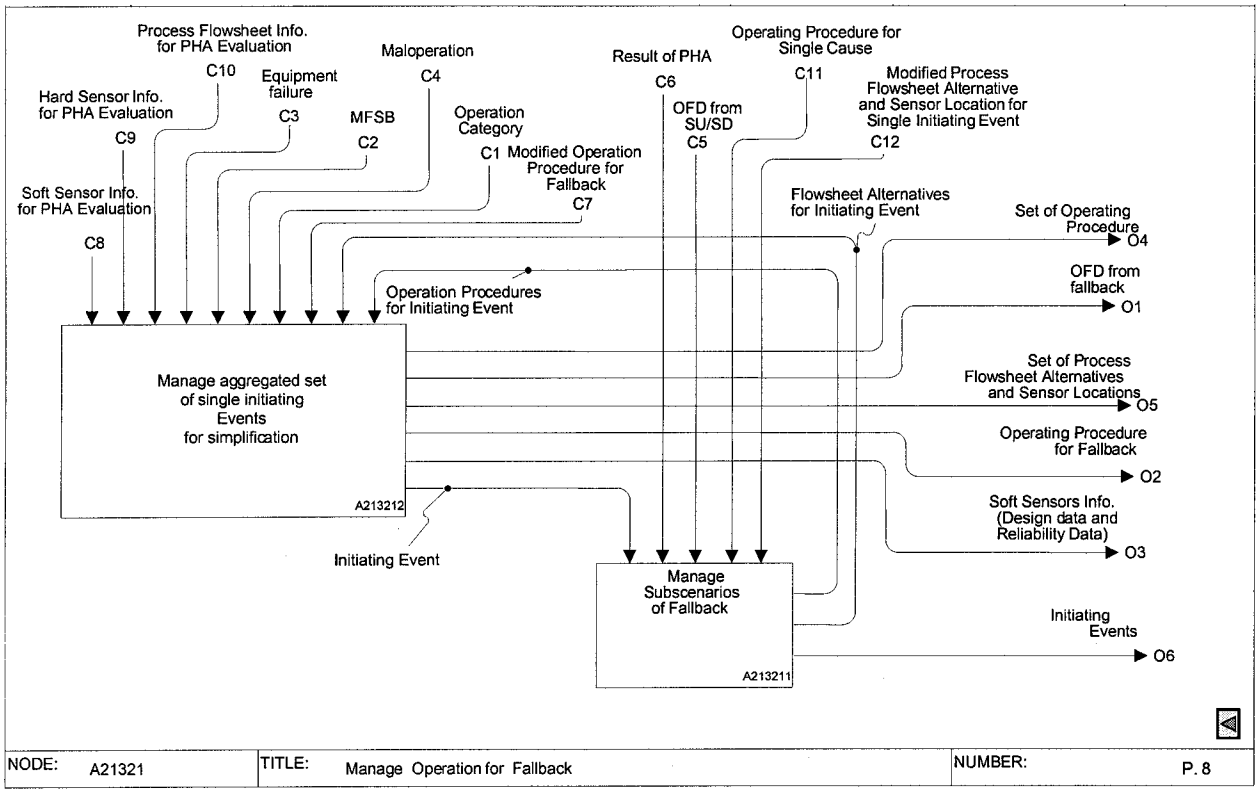

Figure 10: Activity Model – Manage Operation for Fallback (A21321)

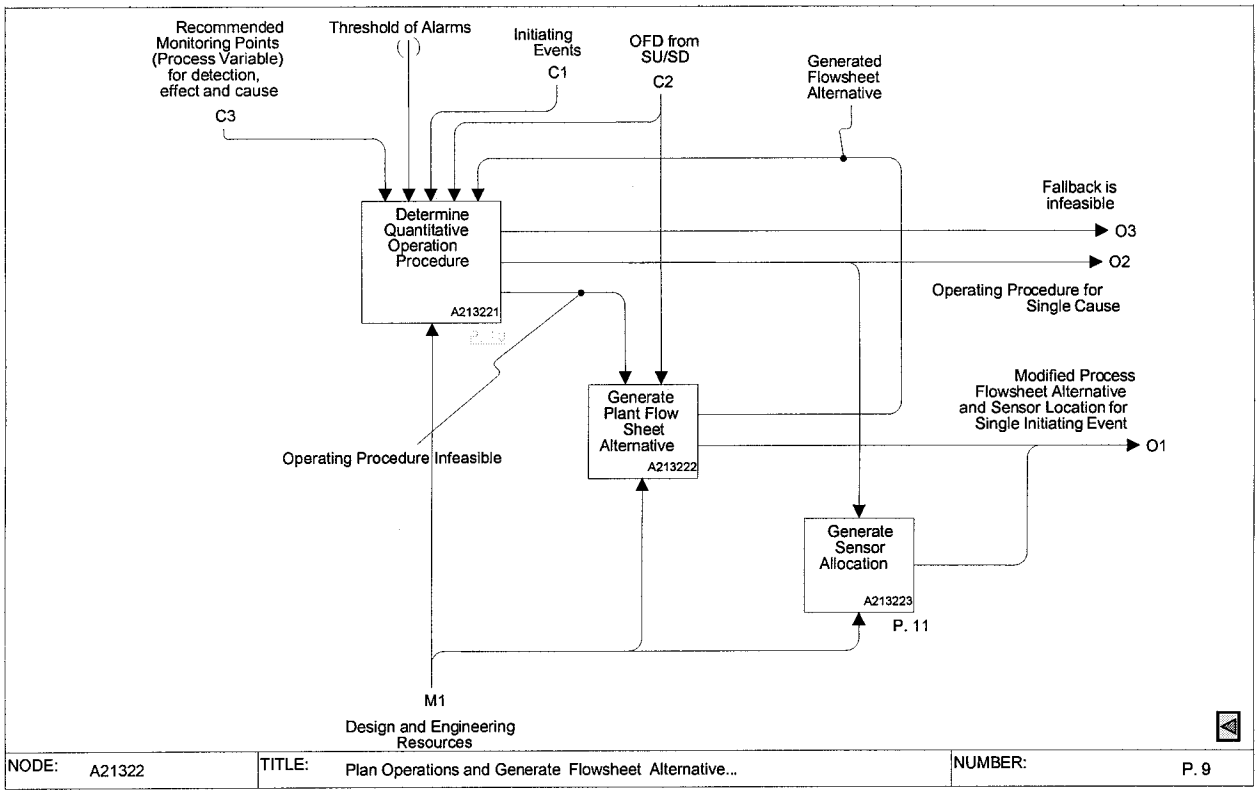

Figure 11: Activity Model – Plan Operations and Generate Flow sheet Alternative (A21322)

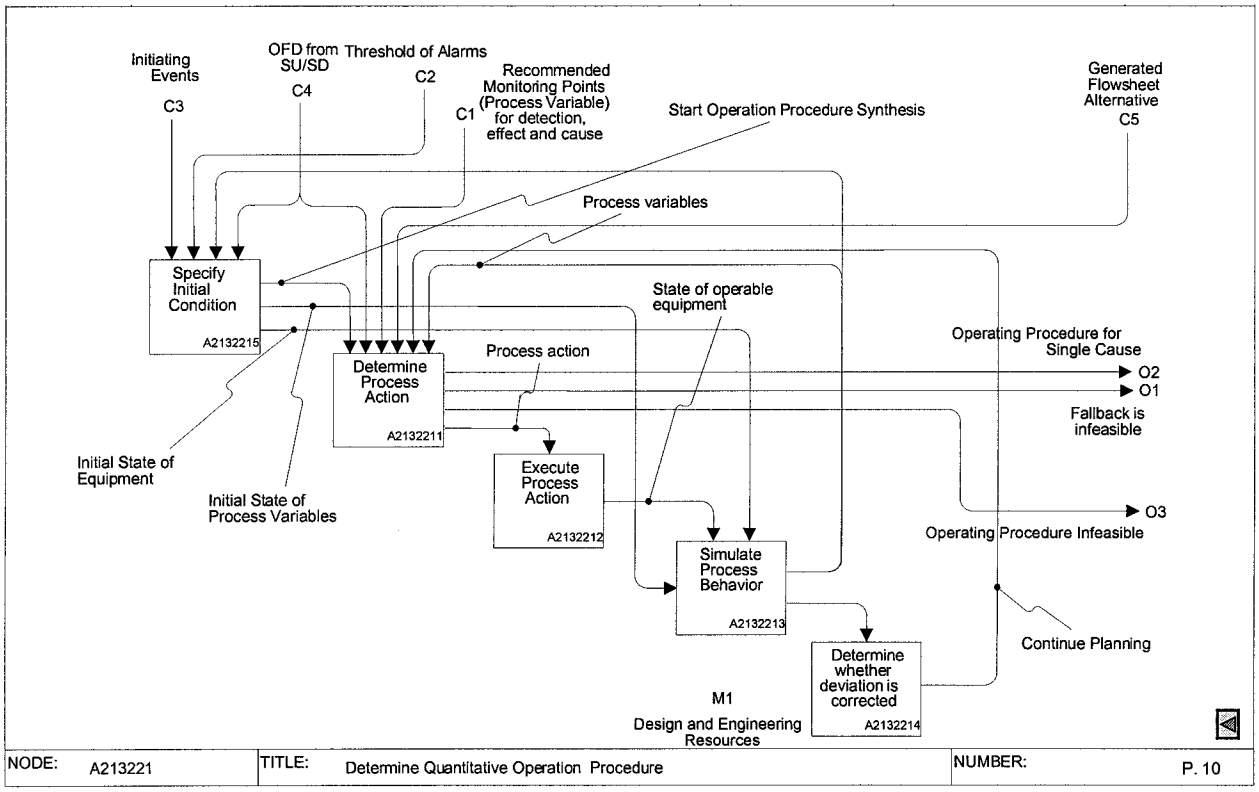

Figure 12: Activity Model – Determine Quantitative Operation Procedure (A213221)

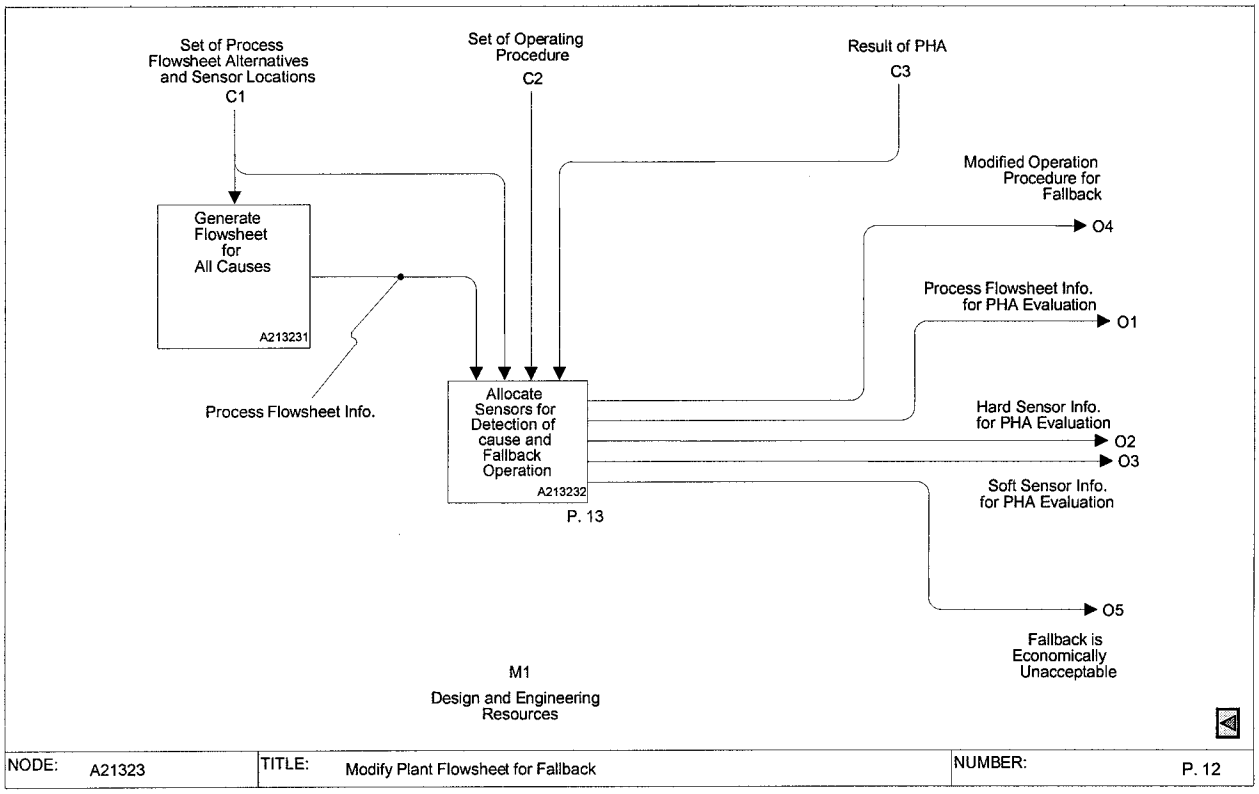

Figure 13: Activity Model – Modify Plant Flow sheet for Fallback (A21323)

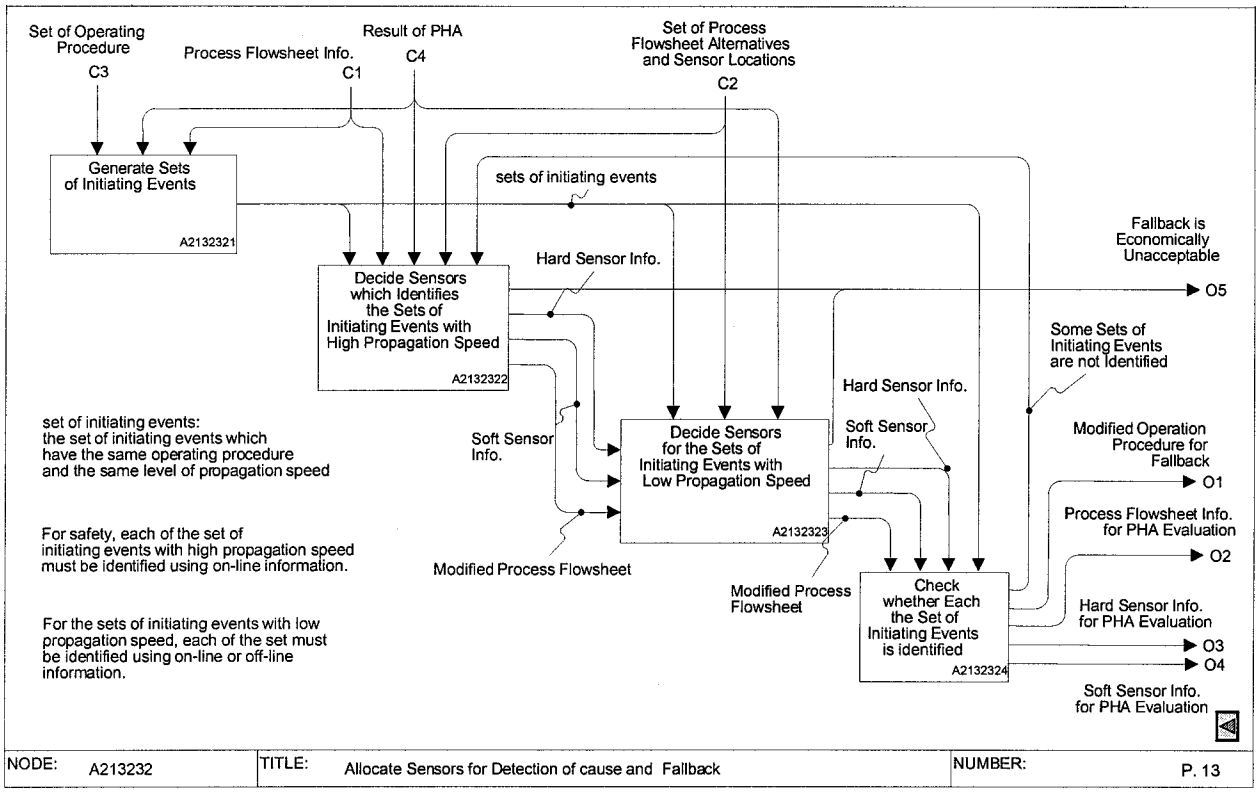

Figure 14: Activity Model – Allocate Sensors for Detection of Causes and Fallback (A213232)