Cumulative Risk Model of Safety Barriers – Case Study

Yasser Fathy Taha, Process Safety Manager, Rashpetco Petroleum, 1 St. No.294, New Maadi, Cairo, Egypt

Abstract

This paper provides a method to develop a dynamic/live operational Cumulative Frequency – Consequence (FN) curve and has focused on an upstream gas production facility (i.e.: the case study) which used to provide about 40 % of the natural gas demand to the National Gas Grid. The case study had some overdue safety critical assurance activities and unavailable and potentially impaired safety systems. The deferral of the safety-critical maintenance is driven by the strategic importance of natural gas supply from the facility to the national gas grid. Without the ability to inspect, calibrate or certify safety-critical equipment, the facility's overall risk level could exceed the Risk Acceptance Criteria (RAC). A structured method was developed to evaluate and communicate the cumulative operational risk to provide an overview of the risk level. The visibility of cumulative risk information encouraged risk discussions before deciding to continue to operate or not with such deferment of Safety-Critical Tasks (SCTs). Bowtie Diagrams (BTDs) were prepared for two Major Accident Hazard (MAH). Risk assessment was performed for two alternatives (performing SCTs within the required/planned intervals and the deferral until the next due date). The impact of deferment of the maintenance activities or the SCTs was evaluated using qualitative and quantitative risk assessment methods. In the qualitative approach, Risk Assessment Matrix (RAM) was used to evaluate the impact of the list of anomalies and degraded performance SCEs. In the quantitative analysis approach, the logical relationships between safety barriers and MAH were described and analysed using Bowtie (BT), Fault Trees (FT), and Event Trees (ET) analysis. FT and BT top event (i.e. Loss of primary containment (LOPC)) is the initiating cause of the ET. The ultimate incident outcome frequency of occurrences at the end of ET was used to develop the operational FN curve of the facility. The Safety barriers model is used to represent MAH scenarios and to describe Safety Critical Elements (SCEs) anomalies. Both barrier model and operational FN-Curve can be used to facilitate the decision-making process and can answer the question, whether it is safe to continue to operate or not?. The results showed that the cumulative risk profile of the case study is still As Low As reasonably Practicable (ALARP) based on the quantitative risk assessment performed using the assumptions and methods in this paper. The results of qualitative risk assessment showed that the cumulative risk profile is no longer ALRAP and immediate actions needed to be taken to shut down the facility and perform the safety-critical Maintenance, Inspection, and Testing (MIT). It is concluded that the cumulative risk profile of the case study is no longer ALARP. The conclusion was based on the qualitative risk assessment process. This paper assessed and described the cumulative notion of risk in two forms. The first form is the traditional safety barrier model using the James Reason Swiss cheese model where multiple failures in the safety-critical systems can cumulatively impact the risk profile of the whole industrial facility. The second form; is a new approach that involves the development of the operational FN-Curve that can represent a long range of accidents in one risk curve at which the cumulative frequencies of having multiple incidents are changed with the change of the SCEs performance. Having a full operational FN curve will represent the live/ dynamic cumulative risk profile of industrial facility where Any change in the performance of the SCEs (due to impairment, deferment of assurance task, or unavailability/ isolation) will lead to change in the incident rate and subsequently will change in the safety barriers performance and the operational FN-Curve.

Keywords

Cumulative risk assessment, Bowtie analysis, Risk management, Barrier Model, safety-critical element management, and Operational FN curve.

Introduction

Accidents happen if multiple barriers fail to perform their intended function. Safety barriers/systems reduced performance will increase the likelihood of an accident. It is important to understand and monitor the status of the safety barriers to ensure that major accident risks at an industrial facility are being suitably managed continuously. It is necessary to maintain safety barriers in an effective state by implementing a list of business processes such as Safety Critical Tasks (SCTs). SCTs can be allocated to / mapped with safety barriers using BT Diagram (BTD) (Stein, et al., 2016).

During the design phase of an industrial facility, Bowtie (BT) analysis is used to identify safety-critical systems which prevent and control the Major Accident Hazard (MAH) scenarios identified in the safety case. BTD can be used to describe the trajectory of all possible consequences of an accidental scenario. Design phase BTD assumes a fixed performance of the add-on engineering barriers - all systems are performing as intended based on the assumption that the safety system operated within its Safe Operating Limits (SOL) and if the assurance tasks aimed to ensure/restore the reliability of the system are executed in the required intervals.

In the operations phase, Safety barriers can experiences faults/failures which can be: (1) Detected or undetected, (2) Within the SOL or out of SOL, and/or (3) Subject to instant adjustment and compensation by a human/operator or not (Stein, et al., 2016). A good practice is to include the Performance Standards requirement into the Computerized Maintenance Management system (CMMS) that manages Maintenance, Inspection and Testing (MIT) of safety barriers therefore all information about SCEs performance are collected, and analysed then appropriate actions can be identified to maintain safe operations. Another good practice is the use of The barrier model to communicate/describe the major accident cumulative risk. In case of any anomalies or degraded performance in safety barriers, Risk reduction can be concluded and achieved by applying interim mitigation measures until the adequate performance of the safety system is restored or recovered.

The “Swiss Cheese” model is a component of the Reason Model of Systems Safety which reflects on the principle of defence in-depth using a set of successive protection layers (i.e. barriers) that prevent hazards from being realized causing accidents (HaSPA, 2012). Safety barriers are presented as cheese slices. The “holes” in the Swiss Cheese slices represent weakened barriers either caused by active or latent failures. Latent conditions or failures interact with active failures (i.e.: action, condition, or inaction) to increase the possibility of having an accident. When the holes in the protection layers align due to active failures, accident happen. The model provides a pictorial display of the sequence of unfavourable events (Stein, et al., 2016). The concept of the barrier model is simple and representative and easy to understand, for that reason, it is widely used and provides detailed insight into the safety barriers (Mehmood, et al., 2015). The cumulative Risk Assessment (CRA) is the evaluation of the overall operational risk which results from multiple adverse effects of the safety barriers performance. CRA aims to assess the ongoing effectiveness of safety barriers; hence assess the increase from the baseline (i.e.: design) risk level.

In 2017, The upstream gas production facility (Figure 1) was almost two years overdue for its planned shutdown for maintenance. The following SCTs list were the main assurance or repair tasks that require total production shutdown to enable maintenance.

(1) Sealine valve replacement – a passing isolation valve on a 36” pipeline. An Emergency Shutdown valve that provides boundary isolation between offshore/subsea wells and onshore facilities. **(2) Regeneration heater inspection** – heater tubes testing was 2 years overdue and requires removing a tube section for examination following 10 years in service according to ASME recommendations**. (3) Cause & Effect Proof Tests** - More than 2 years overdue. **(4) PSVs Calibration and testing** - Some PSVs are no longer within the calibration period.

Methods Summary

The following steps were used to review safety barriers performance in order to assess whether they are adequate or not.

(1) **Identify the List of Unavailable / Impaired SCEs -** Review the facility CMMS to identify impaired/unavailable SCEs and the list of the deferred SCTs.

(2) **Identification of the foreseeable MAH associated with The Unavailable / Impaired Barrier** - Use the facility safety case **(DNVGL, 2015)** and QRA reports **(ADVANTICA, 2008)** to identify the MAH scenarios associated with the impaired SCEs then classify the SCEs into 3 classes based on the SCEs functionality: (1) Can lead to MAH, (2) Mitigate MAH or (3) Control MAH) **(BG, 2012)** then use the Hazard and Operability (HAZOP) and Layer of Protection Analysis (LOPA) studies to develop BTDs. Table-1 proposes a cross-reference between BT, HAZOP, and LOPA terminologies.

LOPA methodology mainly depends on HAZOP data to build up the LOPA scenarios. Cross-referencing / Data Mapping of HAZOP with LOPA is a usual practice used in SIL determination studies. HAZOP develop data for LOPA **(IEC, 2003)**.

(3) **Development of Bowtie Diagrams** Bowtie XP software was used to develop the BTDs. As illustrated in Table-1, HAZOP study data were used to develop BTDs which starts with adding all the primary / main barriers to the BTD according to their sequence of operations in response to specific threats leading to the top event. This step includes adding the following: (1) Barrier Decay Mechanisms which is a fault mode/malfunction mechanism that can lead to failure of the primary barrier and (2) secondary barriers or barriers decay control which is a process or system utilized to prevent/control decay mechanisms of the primary barriers. The final step is to classify the barrier anomalies into 5 classes –(1) Deviation from Barrier Performance Standard, (2) Deferral of Barrier Assurance, (3) Over-rides or inhibits on barriers, (4) Abnormal Plant Operations or/and (5) Human Competency.

(4) Qualitative Risk Assessment - The facility cumulative safety barrier model (Figure-2) consists of 8 hardware barriers that either prevent or control LOPC scenarios. Hardware barriers are not arranged in their sequence of operation in the barrier model. The risk assessment starts by determining the risk Scores using the facility RAM considering the following conditional/if statement: (BG, 2012): (A) If the initial risk score showed a significant increase above the baseline (Design) Risk level (RAM acceptance criteria) and the mitigation measures are partially effective in reducing the risk level, the safety barrier can be classified as red (unacceptable risk level). (B) If the mitigation measures are effective in reducing the risk level to the ALARP region, the safety barrier can be classified as amber (controlled risk level). (C) If the mitigation measures are fully effective in reducing the risk level to the broadly accepted region, the safety barrier can be classified as green and healthy.

The subsequent steps were to investigate the cumulative impact of all risks together and to check potential escalation scenarios / cumulative impact of incident time, incident duration, and relative location. Finally, Evaluate whether the residual risk is ALARP using the risk acceptance criteria (i.e.: conditional/if statement) described previously.

(5) Quantitative Risk Assessment -The following section will describe the quantitative risk assessment approach**.**

5.1 Development of Fault Tree for Prevention Barriers, Layers of Prevention (LOP) or the left side of the BTD. RELIOSOFT fault Tree Analysis software was used to construct the Fault Trees Diagram (FTD). This step aims to determine the LOPC (Top Event) frequency.

5.2 Probability of Failure on Demand (PFD) of Protective Systems – The unavailability, Probability of Failure on Demand (PFD), or Fractional Dead Time (FDT) are all synonymous and representing the protective systems failure to function. (CCPS, 2000**)**. There are two types of failures of Protective systems: (1) Unrevealed failure (function on demand) or (2) Revealed failure. The following section provides the PFD calculations of the two types of failure **(**CCPS**,** 2000**)**.

a. Revealed Failure

One Out OF one (1OO1) combination / system configuration is calculated by Equation (1).

$$\text{PFD} = F \text{ x Repair Time.} \qquad \text{Equation (1)}$$

The PFD is calculated using different equations for different system combinations/configuration (CCPS, 2000).

b. Unrevealed Failure:

$$\text{PFD} = 0.5 \text{ x } F \text{ x Test Interval} \qquad \text{Equation (2)}$$

Where F is the failure rate (y^{-1})

The "hazard or incident rate” (H) can be calculated by Equation 3. (CCPS, 2000)

$$P_{LOPC} = H = D\,x\,\text{PFD} \qquad \text{Equation (3)}$$

Where, D is the demand rate which is Deviations that take the process out of control (CCPS, 2000)

5.3 Development of Event Tree for Protective Barriers, Layers of control (LOC) or the right side of the BTD. Barriers assigned for a specific accidental event should be added to the logic trees in the sequence they will be activated (Hausand, et al., 2004). This step aims to develop the ETD for the right side of the BTD. The initiating event (IE) of the ETD is the LOPC event (top event). In some cases, It may be necessary to use FTA to determine the PFD of Layers of control (LOC) to calculate the failure or success rate of the safety system.

5.4 Operational FN-Curve - A method to develop a dynamic/live operational FN curve is presented in the following section.

In the QRA study, each LOPC scenario has discrete failure frequencies calculated based on the process equipment parts counts. The LOPC frequency is calculated by:

$$F_{LOPC} = \sum n_i f_i \qquad \text{Equation (4)}$$

Where F_{LOPC} is process equipment LOPC frequency (from Process equipment reliability data source)

n_i the number of components i f_i is the frequency of failure for component i.

The mathematics of the FN-Curve was explored in several publications (Ball, et al., 1998) (CCPS, 2009) (I.L. Hirst, 2002) (IChemE, 2009). FN-Curve equation is given as follow:

$$F = A\,(N)^{-b} \qquad \text{Equation (5)}$$

Where, F = Cumulative frequency of N or more fatalities A = constant

b = aversion factor (often between 1 and 2) (CCPS, 2009) N = Number of fatalities

In the developed FTD Figure 8 and 10, The LOPC frequency is calculated based on the PFD of safety systems while QRA data mainly uses the historical failure rate data of process equipment. It is assumed that the calculated FTD frequency (i.e.: LOPC frequency) is equal to or replaces the process equipment failure frequency used in design QRA. The following steps are used to update QRA failure case frequencies using the calculated LOPC frequency: (1) For all MAH scenarios understudy, Use FTD top event (LOPC) frequency (i.e.: Equation-3) instead of the equivalent failure case frequency used in the design QRA study, (2) Calculate the cumulative frequencies of occurrence of all MAH scenarios studied in the design QRA and (3) Plot the updated / operational FN-Curve.

5.5 Risk Calculations

Location Specific Individual Risk (LSIR) is calculated, as follows: (CCPS, 2001)

$$LSIR = F_C . P_{fatality} = P_{LOPC}\ P_{ignition} P_{fatality} \qquad \text{Equation (6)}$$

The Individual Risk Per Annum from flammable effect (yr^{-1}) (IRPA) is calculated as follow: (Franks, 2005) (CCPS, 2001)

$$IRPA = F_C . P_{fatality} . P_{present} = P_{LOPC}\ P_{ignition} P_{fatality} . P_{present}$$

$$= D . \left(\prod_{j=1}^{J} PFD_{i,j}\right) P_{ignition} P_{present}\ P_{fatality} \qquad \text{Equation (7)}$$

F_C = Frequency of the initiating event that gives rise to consequence C

P_{LOPC} is the probability of Loss of Primary Containment D = demand rate (yr^{-1})

P_{FDij} = Probability of failure on demand for the j[th] IPL that protects against consequence C for initiating event i.

$p_{ignition}$ = Probability of ignition of flammable release $p_{present}$ = Probability that individual is present when an event occurs

$p_{fatality}$ = Probability that individual is killed given exposure to the event

PFD for the j[th] IPLs that protects against consequence C for initiating event is given by the: (Pitblado, et al., 2016)

$$PFD_{\ IPLs} = \prod_{j=1}^{J} = \text{PFD}_{\text{ SIB}} . \text{PFD}_{\text{ PCB}} . \text{PFD}_{\text{ ICB}} . \text{PFD}_{\text{ DSB}} . \text{PFD}_{\text{ PSB}} . \text{PFD}_{\text{ SDB}} \qquad \text{Equation (8)}$$

PFD_{SIB} is structural integrity barrier PFD PFD_{PCB} is the process containment barrier PFD

PFD_{ICB} is ignition control barrier PFD PFD_{DSB} is detection system barrier PFD

PFD_{PSB} is the protection system barrier PFD PFD_{SDB} is shutdown barrier PFD

The Emergency response and the lifesaving barrier were excluded from the equation because both are safeguards and not IPLs.

Results and Discussion

As indicated in Table -2, Two main process equipment (Slug catcher and Regeneration gas heater) had impaired safety-critical elements and deferred SCTs. The failure mechanisms studied for the Regeneration gas heater are tube failure or burner management system function failure which may lead to fire or explosion. The heater is overdue 10 years internal inspections for more than 2 years (including coil destructive replica test) therefore the failure potential is increasing. Failure of the heater is one of the MAH scenarios studied in the QRA report. Overheating of the processed natural gas can cause heater tubes to exceed metallurgical limits and rupture. The deferral of internal inspection is a significant issue and needs to be evaluated to understand the impact of delaying the tube/coil inspection especially that there are other latent failures identified on the same process equipment. PSVs of the heater is the last layer of protection against heater over-pressurization. PSVs have a single isolation valve therefore removal of the valve for calibration and testing cannot be performed having a high-pressure end pipe with a single isolation valve which is not permitted condition by the facility safe Isolation procedure.

Having a passing Emergency Shutdown Valve (ESDV) means that ESD function cannot be achieved and flammable hydrocarbons flow from subsea wells cannot be stopped during emergency cases therefore the ESD valve cannot perform its function as a safeguard designed to Mitigate any onshore MAH. The same ESDV is part of a Safety Instrumented Function (SIF) that protects slug catcher and downstream lower pressure rating equipment against overpressure.

Although each Process Hazard Analysis (PHA) technique has its objective and methods, Cross-referencing / Data Mapping between LOPA, HAZOP and BTA Studies was straightforward and simple to implement using Table-1 terminologies that link between the HAZOP (DNVGL, 2015), LOPA studies (DNVGL, 2015), BTDs and FTDs. Figure 3 and 4 provide the BTDs of slug catcher LOPC and Figure-5 and 6 provide the BTDs of regeneration gas heater LOPC. The following list represents some of the differences that are worth highlighting concerning the HAZOP, LOPA, and Bowtie cross-reference/mapping step: (1) Bowtie Analysis has a wider scope and covers more non-process-related threats than HAZOP (the developed BTDs in this paper did not include all the possible threats that can lead to LOPC). (2) HAZOP depends mainly on a systematic approach to cover operability and process hazards. Other failure causes such as technical failures (physical degradation), operational, design, and external events/loads were not included in the BTDs. (3) Bowtie technique is capable to identify and analyse all potential threats that could lead to LOPC while the use of the HAZOP worksheet information to develop BTD can limit brainstorming efforts to identify all possible threats that can lead to the top event.

The benefits of Cross-referencing / Data Mapping of HAZOP, LOPA, and Bowtie data are given below: (1) Provide risk analyst with a simple tool to visualize risk and show interrelationships between the safety protection layers and the management system arrangements/assurance tasks (such as MIT); hence facilitate any further risk assessment activities. (2) The use of the developed BTDs as an aide to ensure better quality and effective Operational Risk Assessment(ORA). (3) Embrace the concept of barrier thinking and primary (Main) and secondary (Support) barriers. (4) Demonstrate the possibility to build up Bowties library for all the MAH scenarios identified by the QRA study. (5) Ability to develop Quantified BTDs by Adding the IPLs PFD to the BTDs

Qualitative Risk Assessment Results

The information extracted from CMMS and the BTDs was used to conduct an Operational Risk Assessment (ORA). The risk scoring using RAM was performed. A list of risk reduction measures and remedial actions (recommendations) were identified. Risk scoring was conducted using RAM for anomalies or degraded performance SCEs. The initial and residual risks were determined. The initial risk scoring was performed without considering existing risk control measures. The residual risk was evaluated as unacceptable risk therefore immediate action needed to be taken to reduce the risk to ALRAP. The ORA information is used to update the safety barriers model qualitatively. The overall risk evaluation of the PCB and SDB is unacceptable while the remaining six barriers are healthy. The Barriers are represented in visual format by colour coding based on their assessed effectiveness. Risk reduction measures were implemented until the performance of safety-critical elements was restored/recovered. All the identified mitigation measures are administrative controls that are either part of an existing management system arrangement or add-on interim mitigation measures established specially to reduce the likelihood of the potential MAH scenarios.

Quantitative Risk Assessment Results

No real-time failure data from the case study was readily available; hence failure data published in the literature were used instead. For an incident to happen there must be a change caused by a demand case (i.e.: initiating cause and enabling factor figures 15 and 16) or Deviation that takes the process out of control followed by multiple failures in the safety systems. The FTA of the left side of BTDs represents the likelihood of having the top event after a threat is revealed and the prevention barriers failed to perform their function on demand. The list of undesired outcomes depends on the success or failure of the protection layers. The main factor in determining the incident path is the time at which ignition occurs (direct or delayed ignition). A series of operations or ETA questions were used to construct the ETDs. The output of ETA is a list of ultimate incident outcomes with frequencies of occurrences. All of the outcomes of the accident produced by ETA are possible and each outcome realization depends on the system reaction to the Incident triggering conditions.

For the heater case study, The demand cases investigated were related to processing/operations upsets. All safety system component's failure frequencies were converted to probabilities except for those responsible for the demand rate. A gate-by-gate calculation performed for normal (alternative 1) and extended (Alternative 2) operational Scenarios/maintenance intervals (Table-3 and 4). The extended interval was 2 years assuming extended continuous operational instead of 1 year. The FT was constructed using the same logic used in LOPA and SIL determination studies (i.e.: layers of protection onion ring diagram). For the two alternatives / operational scenarios, LOPC frequencies were determined and risk was estimated using generic failure rate data of safety system components.

The investigated causes of LOPC is process upset and technical failures (physical degradation). Other failure causes such as design, and external events/loads failures were not included in the FTA. The top event considered in the analysis of the Regeneration gas heater is Coils damage leading to LOPC (Figure 10). The FTD was constructed top-down. 3 types of damage which required to be controlled and monitored are coil thickness reduction, cracking, and Metallurgical changes. A Heater Tube Assessment was conducted and the frequency of failure of the tube was determined using the API 581 method (API, 2000) Appendix J to determine the Probability of Failure based on the following factors: (1) The type of inspections performed and (2) Heater Operating hours.

Table-3 provides the gate-by-gate calculations of FTD of the two operational alternatives. The calculated LOPC frequency is 2E-06 / year for performing the internal inspection after 12 year's in-service and proof testing of overpressure/temperature protection SIF (operational scenario1). for operational scenario 2, the LOPC frequency is 8,4E-06/ year.

The objective of ET is to determine the ultimate incident outcomes frequency. The calculated LOPC frequency is used as ETD initiating event frequency. The Inspection effectiveness reduction factor was found as the main controlling factor in the failure rate change. Two types of inspection were considered to reflect the inspection plan effectiveness. Highly effective inspection which represents the performance of inspection within the required intervals and ineffective inspection which represents the lack of inspection due to the heater's unavailability for maintenance. The extended continuous operating time without testing the coils was 13 years. It was observed that the probability of failure of the heater coils will not increases dramatically by increasing the operating hours as long as the creep critical temperature is not exceeded. The most critical factor in increasing the probability of failure was the effectiveness of the inspection regime used to judge the coil integrity.

For the slug catcher case study, The threat considered in the LOPC assessment was overpressure caused by blocked outlet case or pressure shock. (Sklet, et al., 2015). The pressure rises in the slug catcher in case the offshore control system failed to close wells on demand, followed by failure of the trip mechanism onshore. Table-3 provides the gate-by-gate calculations of FTD of the two operational alternatives. The calculated LOPC frequency is 7,5E-06/ year for the operational scenario1 while for operational scenario 2, the LOPC frequency is 4,2E-05 / Year.

ETDs for Slug catcher LOPC are given in Figures 11 and 12. ETDs for Heater Coils LOPC are given in Figures 13 and 14. The ETDs list the layer of protection of the BTDs and determines the likelihood of having the ultimate accident consequence. The final state of the ETD provides the frequency of the possible undesired outcomes. The undesired outcomes are harmless gas release, jet fire, and explosion for both accidental scenarios under study. The highest incident outcome frequency leads to a fire or explosion used to develop the operational FN-Curve of the case study.

Risk Calculations

Risk is Tolerable if ALARP. The case study Individual Risk criteria are given in Table 5. (DNVGL, 2015) The Total Potential Loss of life (PLL) values are equal to the area under the FN-Curve and both represent the expected number of deaths associated with a list of scenarios (i.e.: group risk). (J.K.Vrijling, et al., 1997). Table 6 provides the PLL for all MAH scenarios, updated LSIR for the 2 accidental scenarios under study. The IR evaluation against Risk Acceptance Criteria (RAC) is presented in the following section:

(1) Risk Evaluation Against Maximum Risk Criteria: For a hypothetical individual who is always present in the location, the RAC is less than 1E-03 Fatality/Year. The Calculated LSIR for alternative 2 increased by more than 1 order of magnitude compared with alternative1 but the risk value for the two alternatives/operational scenarios are still below the intolerable criteria of LSIR (using single incident data and for hypothetical person).

(2) Risk Evaluation Against Individual-Specific Individual Risk: A more realistic estimate of risk is the IRPA which is the risk imposed on the individual taken into consideration being at work for a definite time and at several locations. The risk acceptance criterion is less than 1E-03 Fatality/Year. The calculated IRPA for alternative 2 increased more than 1 order of magnitude than alternative 1 but the risk value for the two alternatives are still below intolerable criteria of IRPA (this only using single incident data while the individual/ worker will be exposed to a list of potential incidents being at several locations for a different duration.

(3) Risk Evaluation Against Target Risk Frequency (Occurrences Per Year, Per Event): a measure of maximum risk per scenario that the company will tolerate (CCPS, 2001). The target risk reduction frequency for a Single event that involves 1 to 2 fatalities is 1E-05 (Occurrences per year, per event). The Calculated frequency of consequences (Fc) For alternatives 1 and 2 are 5,2E-06 and 1,4E-06 (Occurrence/Year Event) respectively; which is less than 1E-05 (i.e.: the facility targets tolerable risk frequency for an incident with the potential to cause 1 fatality or 2 fatalities is 1E-05 occurrence/ year. event)**.** For the deferral of safety-critical maintenance until the next due date (Alternative 2), The Calculated frequency of consequences (F_c) for the two studied MAH scenarios will Increase to be (2,9E-05 occurrence/ year event) for slug catcher case which does not comply with the facility target tolerable risk frequency for an incident with the potential to cause 1 or 2 fatalities. For the heater case, the calculated Fc is 5,8E-06 occurrence/year which is still below the target tolerable risk frequency. PFD for each IPL is utilized to update the BTDs of the two MAH scenarios. Figures 15 and 16 give the QBTDs.

For the slug catcher LOPC scenario, the frequency of having jet fire exceeds the company target risk reduction frequency but LSIR and IRPA still comply with risk acceptance level, thus remedial actions need to be taken to reduce the risk by reducing the frequency of the incident but the current risk level is deemed to be insignificant/ tolerable based on IRPA and LSIR acceptance criteria. The safety barrier model of the industrial facility understudy was updated with the aid of the developed QBTDs. The safety barrier model has two barriers (PCB and SDB) in amber colour (risk is controlled and within ALRAP zone).

Operational FN-Curve

The total PLL is not a criterion to make judgments about levels of risk but it is the numerical representation of FN-curve and its valuable inputs when comparing between two alternatives. The PLL for the For slug catcher case LOPC is 1,47E-05 Fatalities/year compared to 7,47E-06 Fatalities/year and ***For the heater tube LOPC,*** PLL is 1,03E-05 Fatalities/year compared to 2,50E-06 Fatalities/year**.** Cost benefits analysis between the 2 alternatives will not be feasible to demonstrate the tolerability of risk to decision-makers as The main driver to continue to operate the facility while postponing the safety-critical maintenance is the importance to continue to provide gas supplies from the facility to the National Gas Grid and not involve monetary aspect.

Figure 17 gives the facility design FN-Curve showing RAC (ADVANTICA, 2008). The calculated incident frequencies in Table-6 are used to update the design FN-Curve. As shown in Figure 18, the risk is increased by one order of magnitude in case action is taken to perform the safety-critical maintenance (operational scenario 1). Both alternatives are still below the design risk curve / Risk Acceptance Criteria (RAC). Figure 18 provides the updated operational FN-Curve. The risk will be increased in case no action is taken to perform the safety-critical maintenance (operational scenario 2) however both alternatives are still below the cumulative RAC. The possible reasons for the difference between the operational and the design FN curve are (1) Conservative failure rate data used in the QRA study, (2) Conservative LOPA targets used in determining the SIL of the safety functions. The method in this paper can be used to evaluate the operational risk level of industrial facilities.

Conclusion

The relationship between the Swiss Cheese Model or the theory and the safety barriers model or the practice was demonstrated in the method and the results sections. Latent Conditions or failures that can lead to degraded performance (i.e.: holes in the Swiss Cheese) could immediately lead to the incident if action (s) or inaction (s) (i.e. Active failure) occurred. Latent failures in one or more Safety Critical Elements (SCEs) will increase the possibility of having accidents. If the SCEs anomaly is not detected and restored to its original performance, active failures, usually caused by human action or inaction, will complete the mission of releasing the beast!. The Safety barriers model utilized to represent MAH scenarios potential and describe Safety Critical Elements (SCEs) anomalies. The Bowties and the safety barriers model provide a pictorial display of the conditions of the safety systems and a trajectory of potential incidents that could happen due to the list of SCEs anomalies. In Bowties, the safety barriers which could prevent and control the LOPC are primary technical barriers that have decay mechanisms controlled by secondary barriers. The secondary barriers prevent and/or detect the technical barriers decay or failure (Human/ operator and Management System).

The safety systems conditions in the upstream natural gas facility understudy suffered from a reduced performance which has proven to increase the likelihood of having an accident and subsequently increase the facility risk profile. The review of the CMMS showed that one of the main process equipment (a gas heater) is overdue internal inspection. Another main process equipment (slug catcher) has an isolation valve with impaired functionality. Bowtie diagram can represent a single MAH scenario while the safety barrier model can represent the cumulative risk profile. Bowtie diagrams were developed for the two accidental scenarios and were used to describe the trajectory/path of all possible consequences. The developed Bowtie diagrams were used in the qualitative risk assessment. Using personal judgment with the aid of RAM, initial and residual risk scores were determined and a list of recommendations were identified and implemented.

In the quantitative risk analysis approach, the logical relationships between safety barriers and MAH were described and analysed using BT, FT, and ET analysis. The hazard rate is the rate of having LOPC and the ultimate incident outcomes are the lists of possible unwanted events that might happen in the case of LOPC. Failure frequencies of SCEs subsystems and components converted to probabilities. FTA quantification was performed. FT and BT top event (i.e. LOPC) is the initiating cause of ET which is used to determine the ultimate incident outcome frequency. The results of qualitative risk assessment showed that the cumulative risk profile is no longer within ALRAP and immediate actions need to be taken to shut down the facility and perform the safety-critical Maintenance, Inspection, and Testing of the impaired SCEs.

Combining fault tree and event tree is the numerical solution of the bowtie model. Two hazard or incident rates were calculated for two operational scenarios/alternatives. The updated incident rate indicates the actual state of the safety barriers taken into consideration any defects or impairment conditions. The ultimate potential accident frequencies were determined and then used to update the QRA failure case frequencies and the design FN-curve. Potential Loss of Life was calculated to update the case study safety barriers model. The updated operational FN-curve and barriers model can be used to facilitate decision making and can answer the question, whether it is safe to continue to operate or not? The results showed that the cumulative risk profile of the case study is still ALARP based on the quantitative risk assessment performed using the assumptions and methods in this study.

The method used in this paper provided links between FTA, ETA, and BTA, safety barriers model, and FN curve. The link between these different risk assessment tools/ techniques will improve the SCEs management and the day-to-day operations safety and will enable the development of a dynamic/ live cumulative safety barriers model.

The cumulative notion of risk was described and assessed in two forms. The first form of cumulative risk representation is the traditional safety barrier model using the James Reason Swiss cheese model where multiple failures in the safety-critical systems can cumulatively impact the risk profile of the whole industrial facility. A second form is a new approach which is the operational FN-Curve that can represent long-range of accidents in one curve where the cumulative frequencies of having multiple incidents are changed with the change in the SCE performance. Having a full operational FN curve will represent the live/ dynamic cumulative risk profile of industrial facility where Any change in the PFD of the SCEs (due to impairment, deferment, or unavailability/ isolation) will lead to change in the incident rate and subsequently will change in the safety barriers performance and the operational FN-Curve. The method used in this paper can be expanded to cover all hazard scenarios of industrial facilities and can be used to generate a concise and representative picture of the cumulative risk profile.

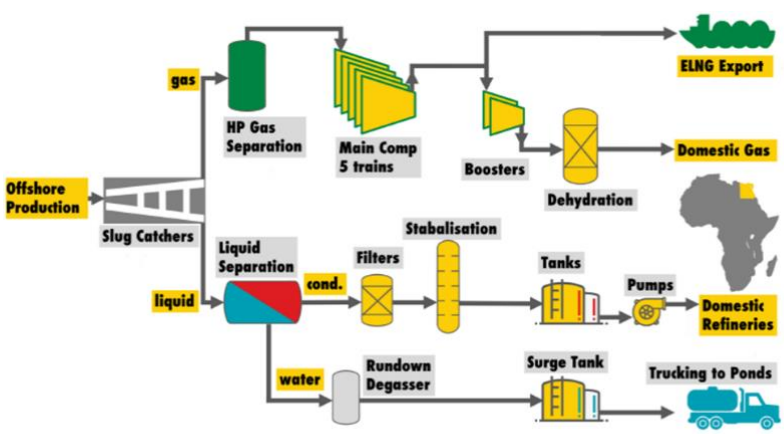

Figure 1: Process Schematic of the Industrial Facility (DNVGL, 2015)

Table 1: Link between Bowtie, HAZOP, and LOPA Terminologies

BT terminology	HAZOP terminologies	LOPA terminology (ies)
Threat	Deviation + possible causes	(Initiating event +Enabling event)
Barrier	Existing Safeguard / Additional Safeguard (Actions) [1]	Protection layers[1]
Consequences	Consequences	Impact event + Severity level
Hazard	Design intent	Description of the scenario

Note1: Not all safeguards are Independent Protection Layers (IPLs), but all IPLs are safeguards (CCPS, 2001)

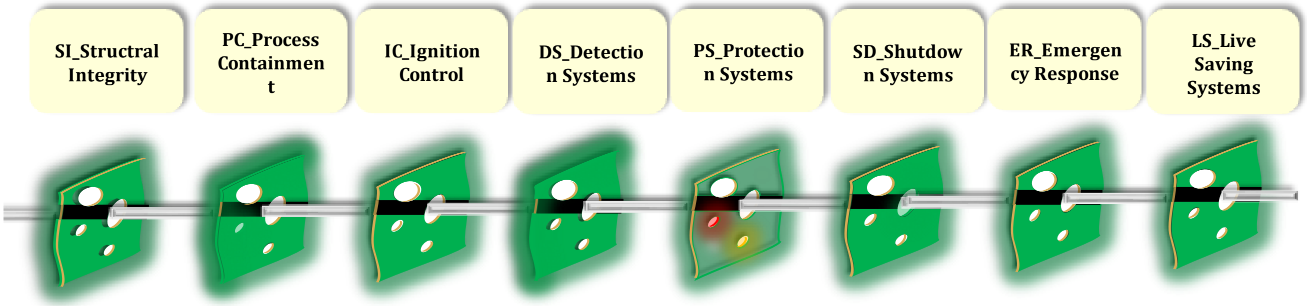

Figure 2: Barrier Model (BG, 2012) (Blacklaw, et al., 2011)

Table 2: List of Equipment and Associated Barrier Anomalies

Equipment Tag	Barrier Anomalies (Yes / No)				
	Deviation from PS[1]	Deferral of SCT	Over-rides or inhibits	Abnormal Operations	Human Resources /Competency
Regeneration Gas Heater	No	Yes	No	No	No
Slug Catcher ESDV	Yes	Yes	No	No	No
Heater & slug catcher PSVs	No	Yes	No	No	No

Note: 1. Deviation from Performance Standard - Deviation to perform intended functi

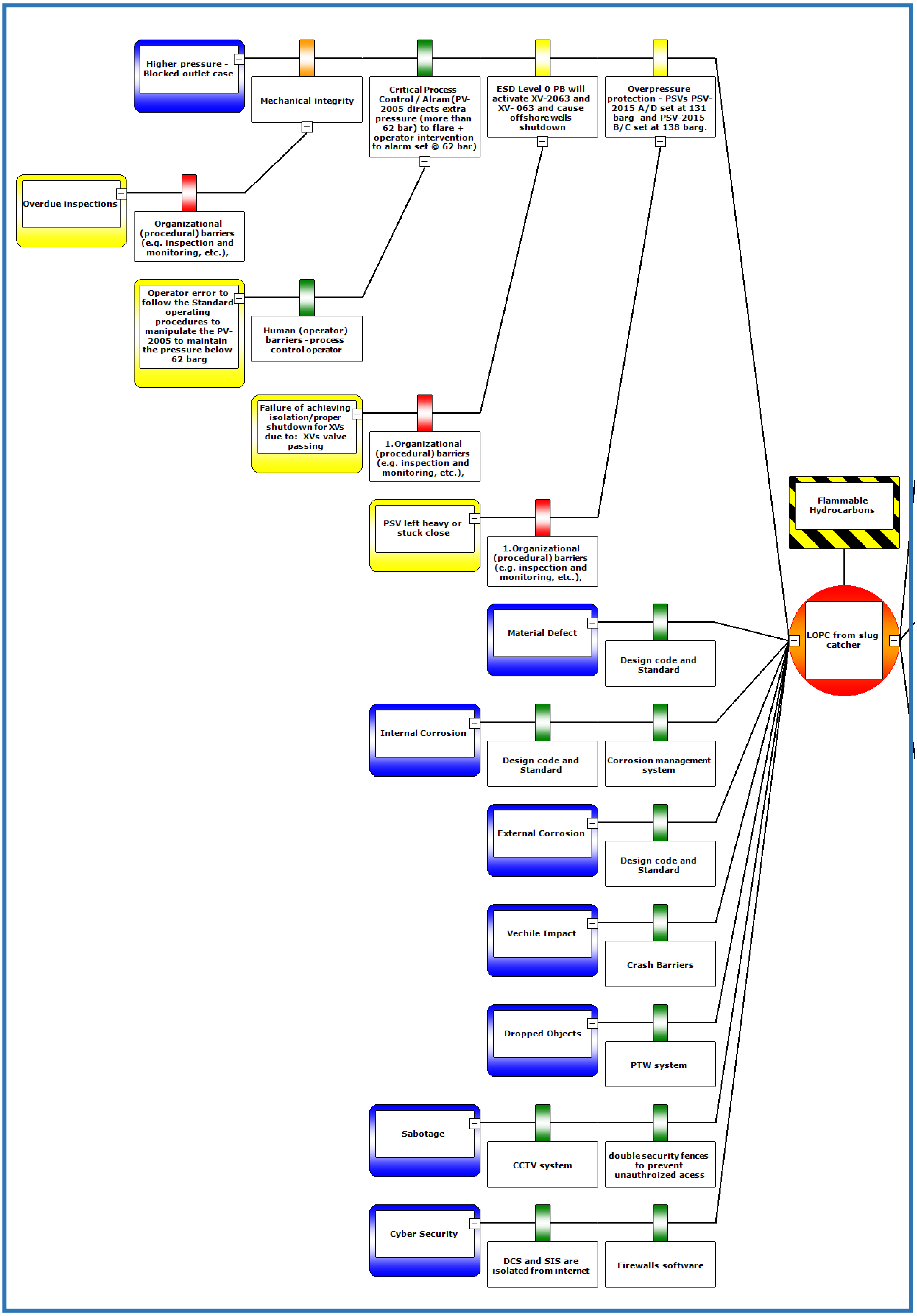

Figure 3: BTD of LOPC from Slug Catcher

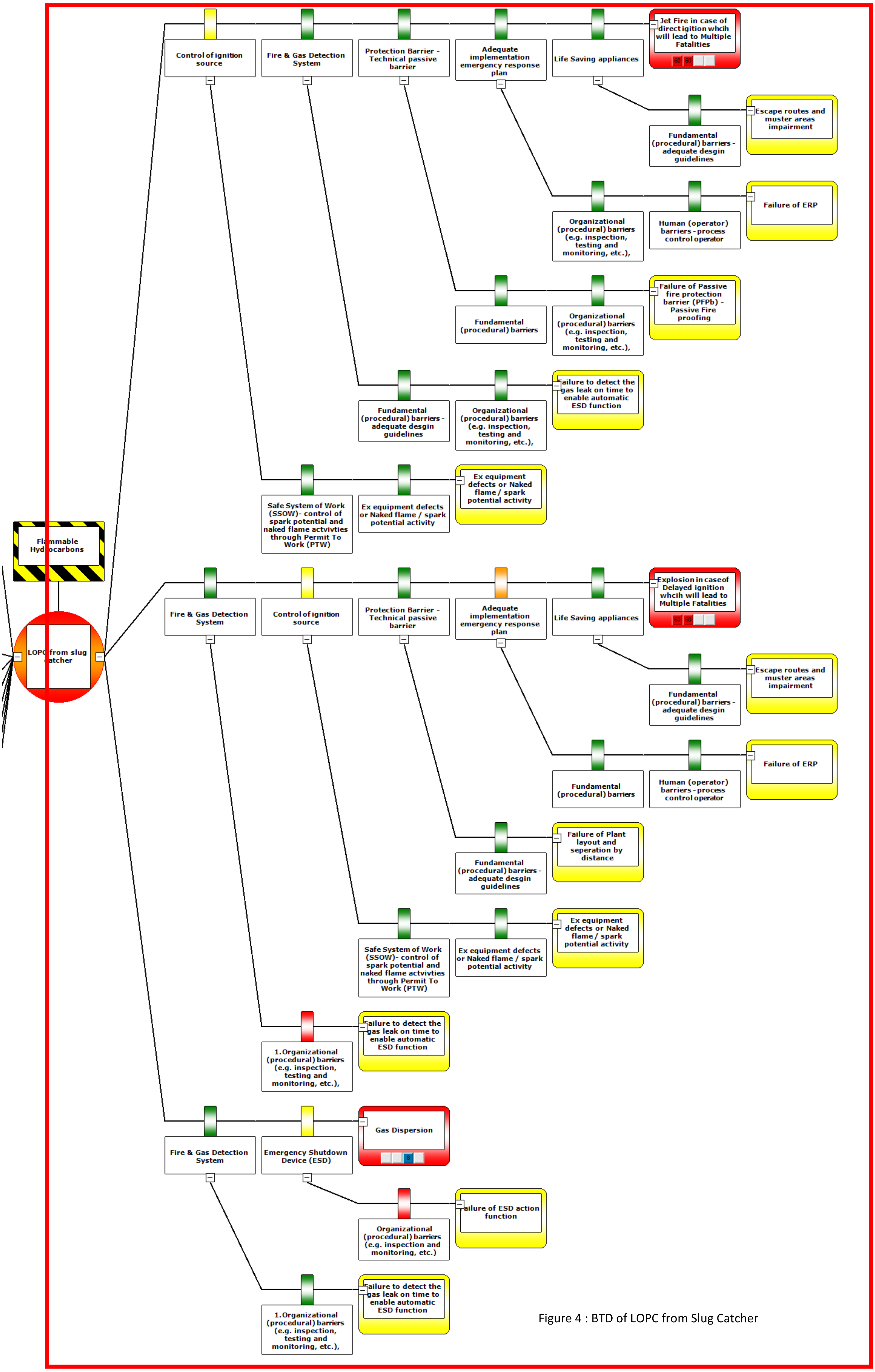

Figure 4 : BTD of LOPC from Slug Catcher

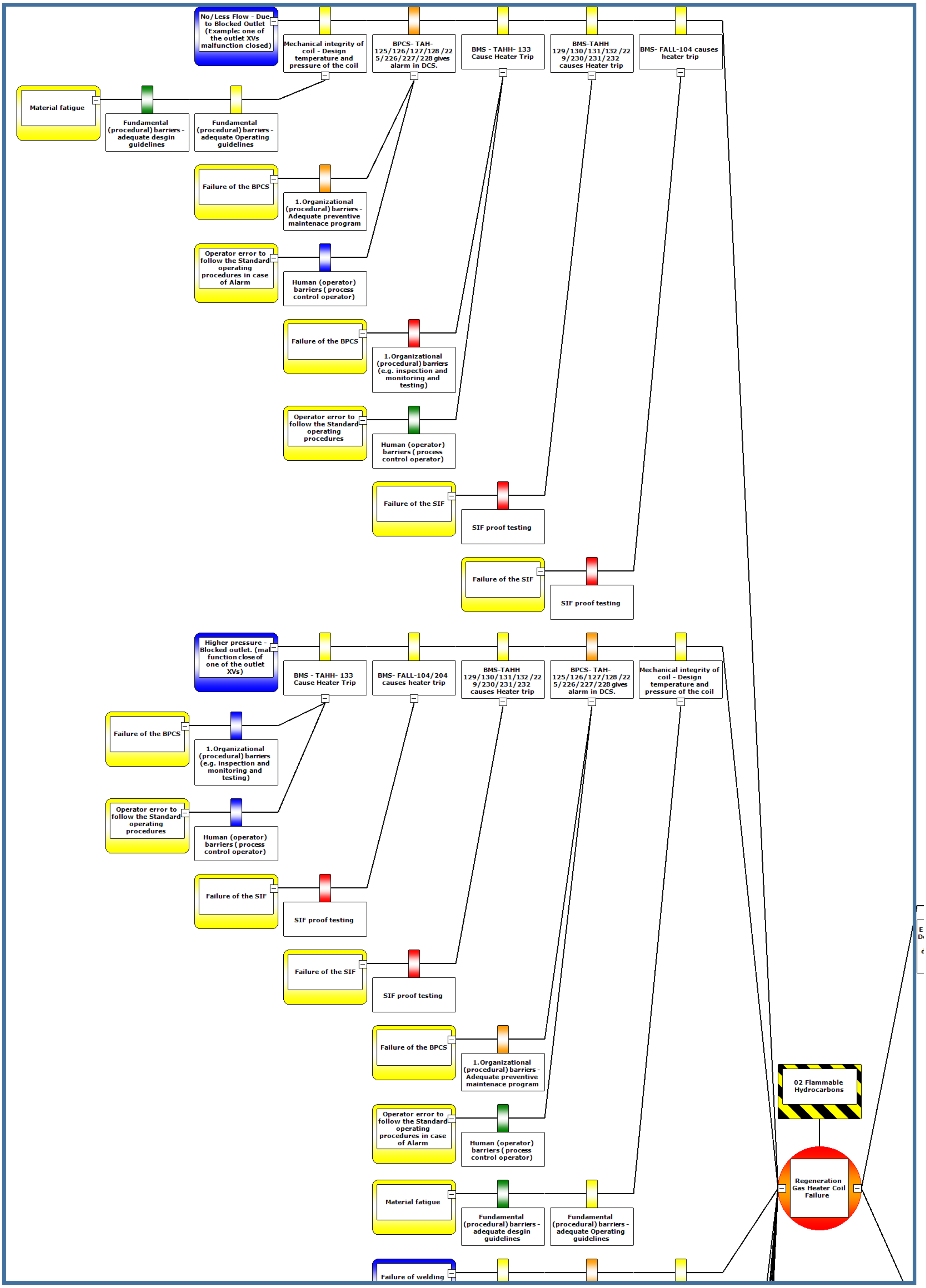

Figure 5: BTD of LOPC From Gas Heater – - Layers of Prevention Set (A)

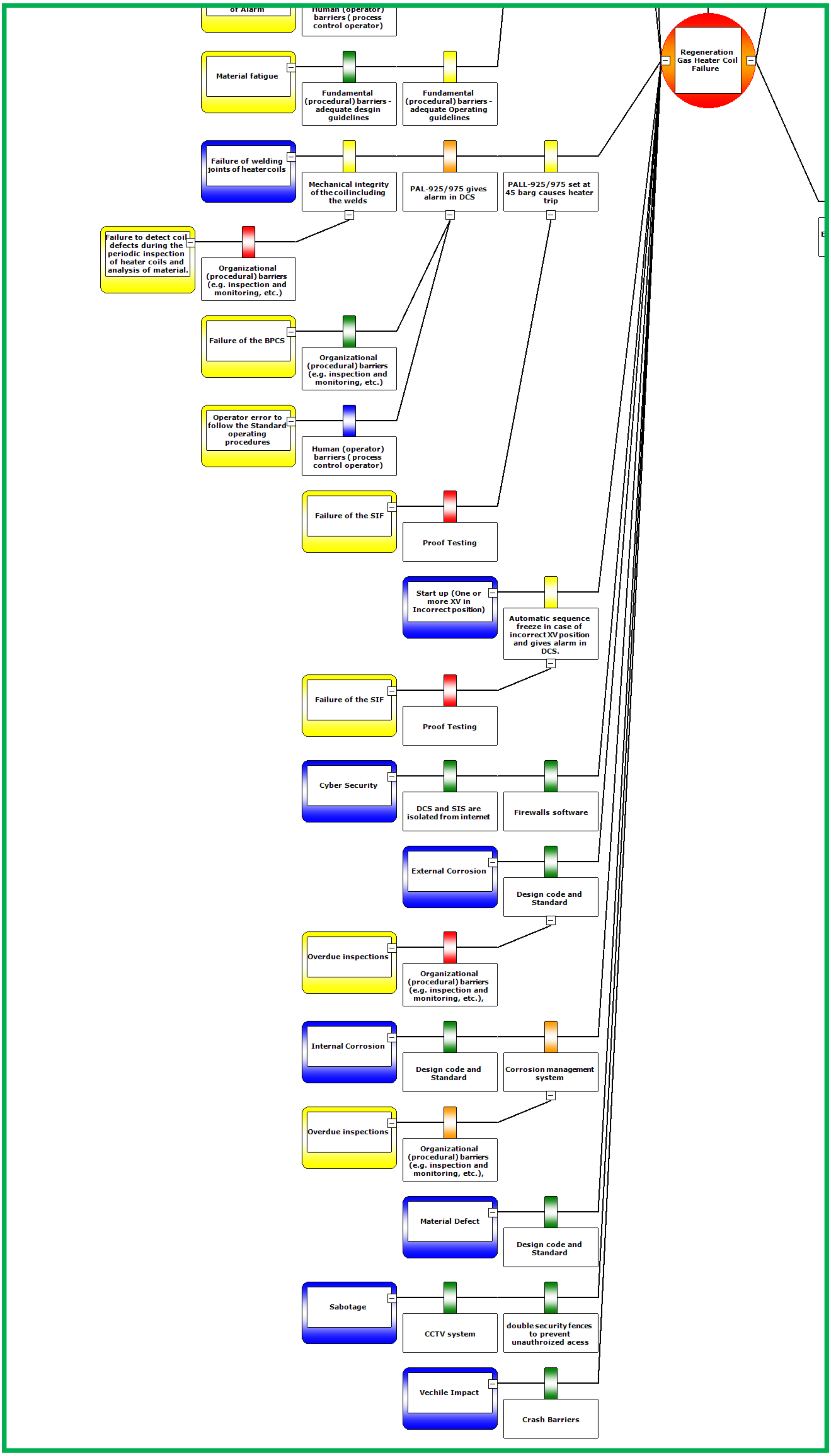

Figure 6 : BTD of LOPC From Gas Heater - Layers of Prevention Set (B)

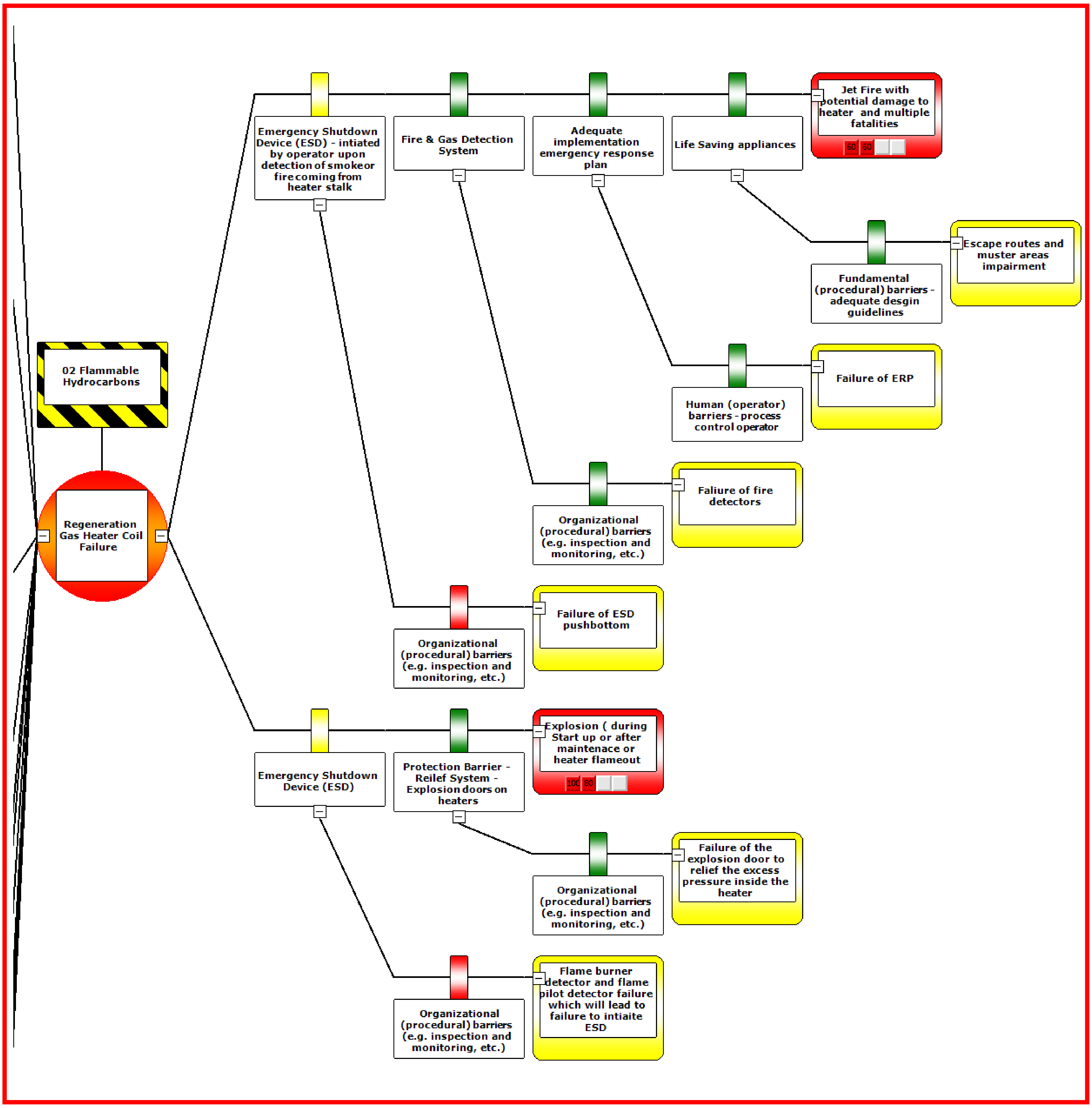

Figure 7: BTD of LOPC From Gas Heater – Layers of Control

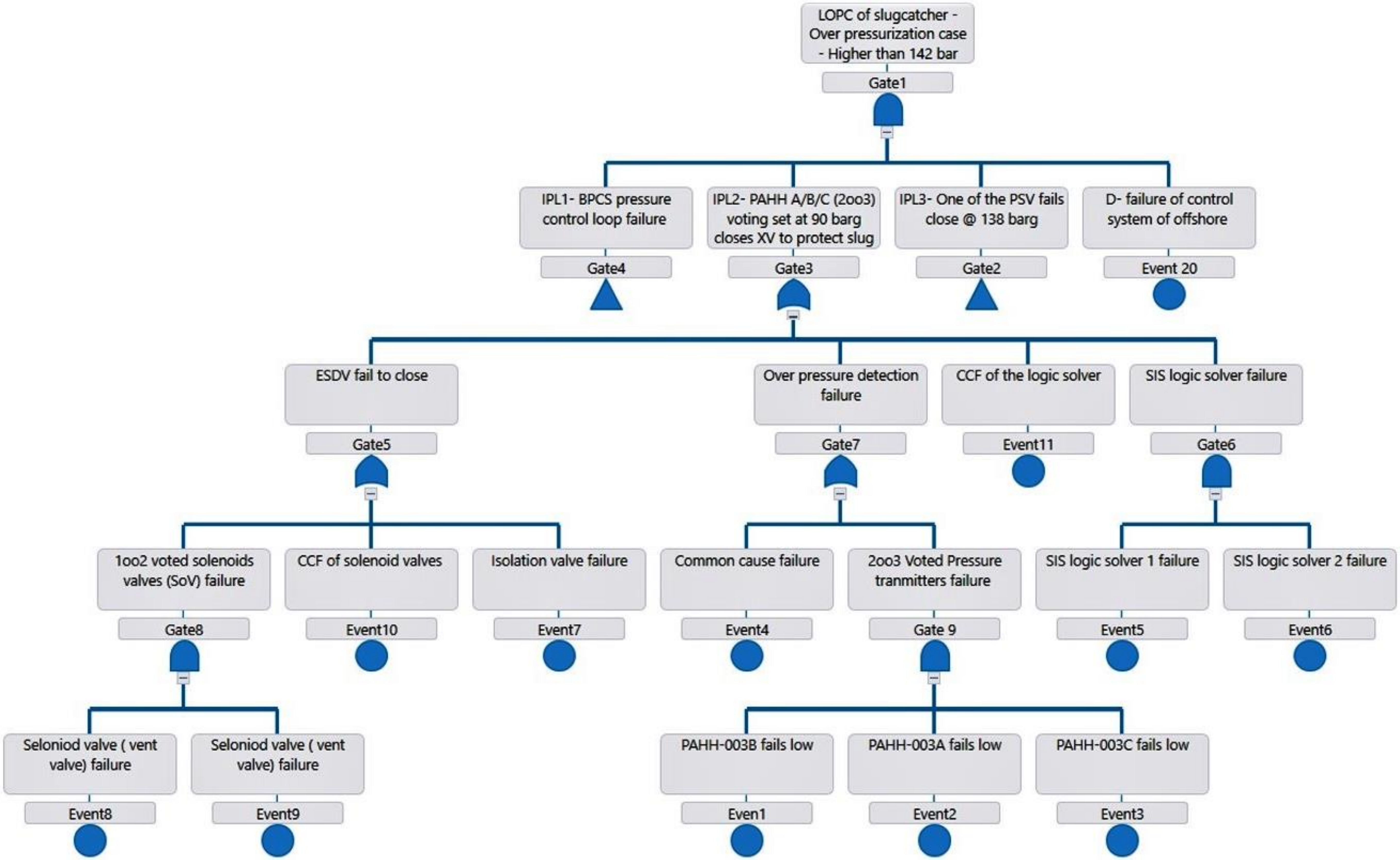

Figure 8: FTA LOPC slug catcher

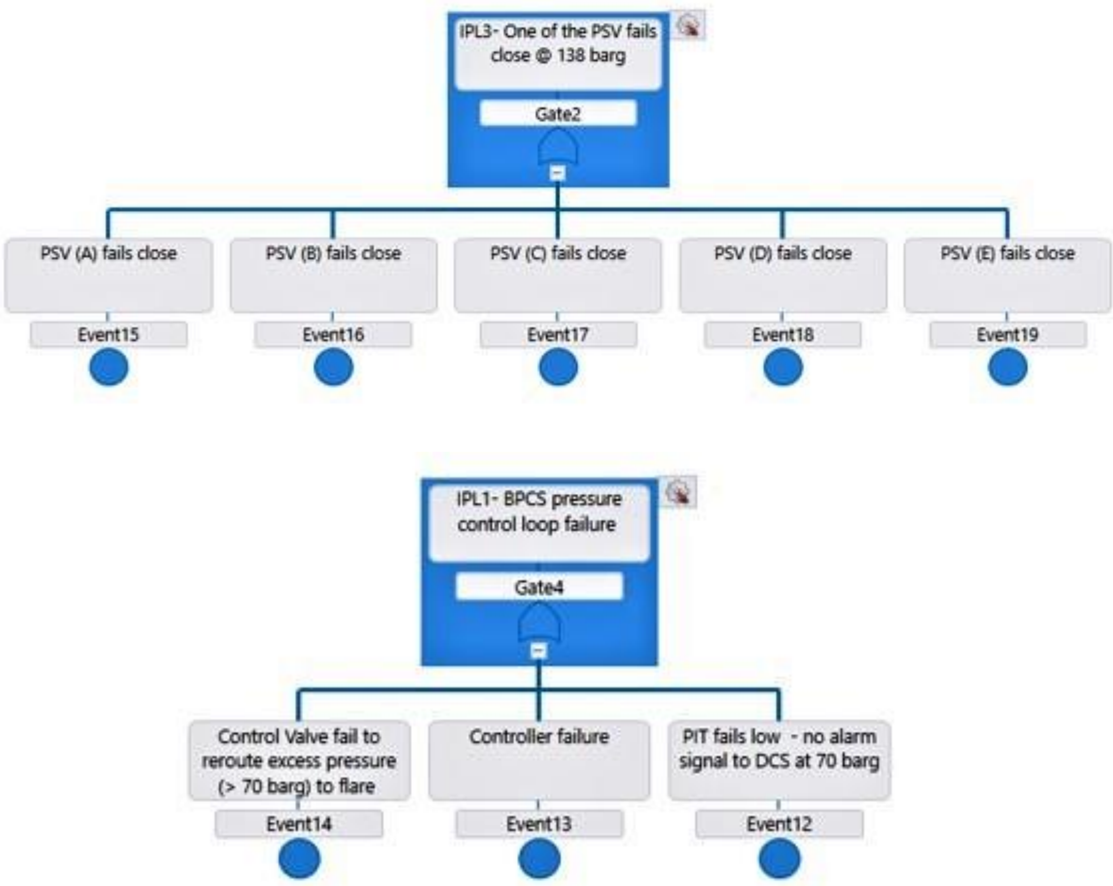

Figure 9 : FTA LOPC slug catcher – Transfer Gates details

Table 3: Gate by Gate Calculations of Slug Catcher LOPC FTD

Gate	Type	Description	Equation	LOPC frequency (Per /year)	
				SD for maintenance	**Extended operations**
1	And	PCB failure - Over pressurization case Higher than 142 barg	P(G2) X P(G3) X P(G4) X P(E20)	7,52E-06	4,20E-05
Gate	**Type**	**Description**	**Equation**	**Probability assuming annual test interval1,2**	**Probability assuming 2 years test interval1,3**
2	Or	IPL3- One of the PSV fails close	P(E17) +P(E18) +P(E15) +P (E16) +P (19)	5,00E-02	1,00E-01
3	Or	IPL2- Failure of PAHH A/B/C (2oo3) to closes ESDV	P(G5) +P(G6) +P(G7) + P(E11)	9,30E-03	1,88E-02
4	Or	IPL1- BPCS pressure control loop failure	P(E12) + P(E13) + P(E14)	1,62E-01	2,24E-01
5	Or	ESDV Valve fails to close	P(E10) + P (E7) +P(G8)	8,83E-03	1,77E-02
6	And	Voted (1OO2) SIS logic solver failure	$\left(\frac{1}{3}\right)\lambda^2T^2$	2,30E-06	9,21E-06
7	Or	Over pressure detection failure	p(G9) + P(E4)	4,00E-04	8,97E-04
8	And	1oo2 voted solenoids valves (SoV) failure	$\left(\frac{1}{3}\right)\lambda^2T^2$	3,10E-05	1,24E-04
9	And	Voted (2OO3) Pressure transmitters failure	λ^2T^2	4,91E-05	1,96E-04

The calculated leak frequency is 7,52E-06 for 1-year testing interval.

The calculated leak frequency is 4,20E-05 / Year for 2-year testing interval.

The calculated leak frequency used as initiating event frequency for the ETDs Figure 11 and 12.

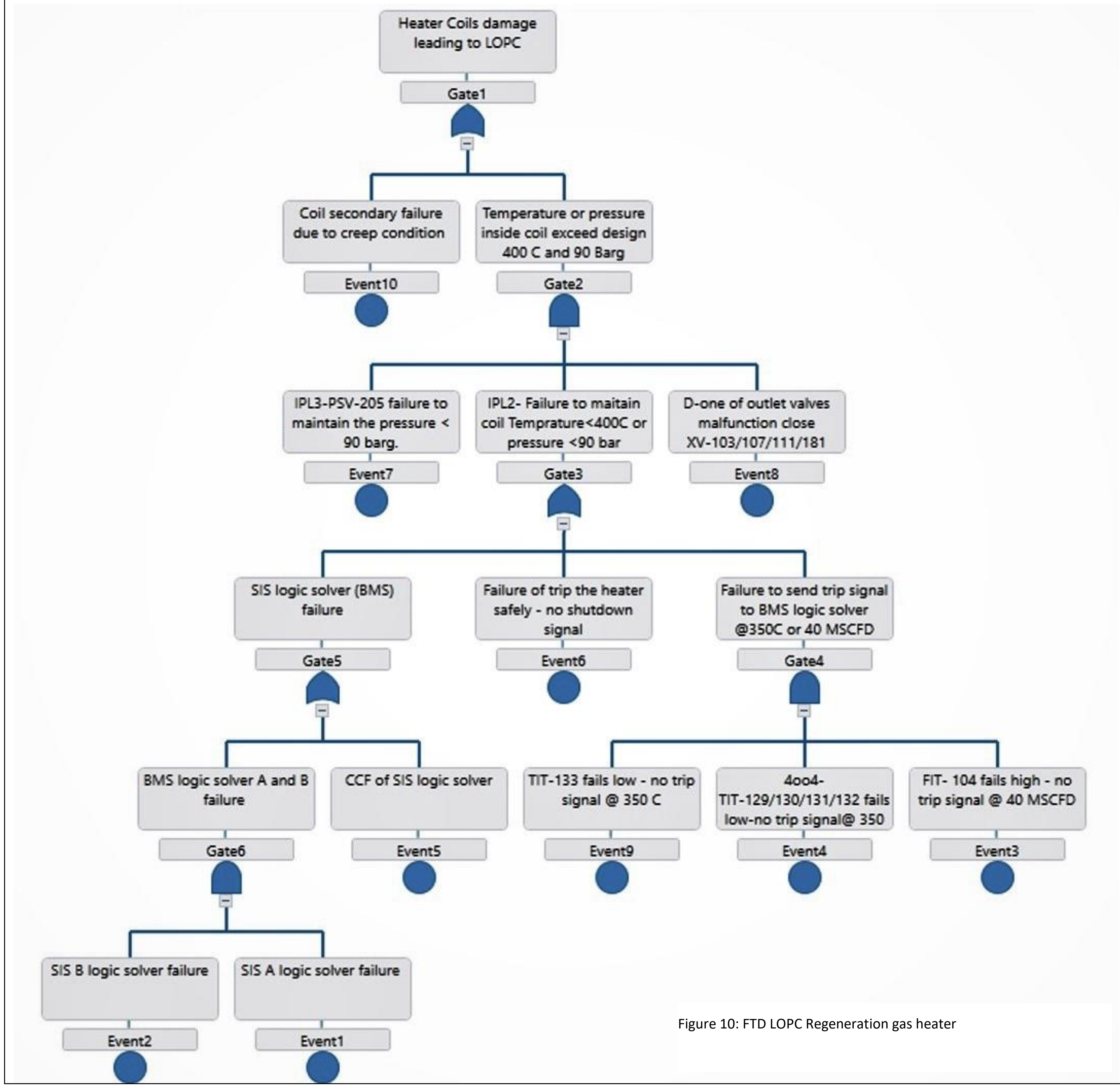

Figure 10: FTD LOPC Regeneration gas heater

Table 4: Gate by Gate Calculations of Leakage Probability from Gas Heater

GATE	Type	Description	Equation	LOPC frequency **(per year)**	
				SD for maintenance	**Extended operations**
Gate1	Or	Coils damage leading to LOPC	P(G2)+P(E10)	2,04E-06	8,39E-06
GATE	**Type**	**Description**	**Equation**	**Probability after 12 years in service**	**Probability assuming 20 years test interval**
Gate2	And	Temperature or pressure inside coil exceed design 400 C and 90 Barg	P(G3) X P(E9) X P(E9)	1,91E-06	7,66E-06
Gate3	Or	IPL2- Failure to maintain coil Temperature<400C or pressure <90 bar	P(G5) +P(G4) +P(E6)	1,82E-03	3,64E-03
Gate4	And	Failure to send trip signal to BMS logic solver @350C or 40 MSCFD	P (E3) X P(E4)X p(E7)	2,47E-07	1,98E-06
Gate5	Or	SIS logic solver (BMS)failure	P(G6) + P(E5)	6,74E-05	1,38E-04
Gate6	And	BMS logic solver A and B failure	P(E1) X P(E2)	1,73E-06	6,91E-06

A	B	C	D				
Initiating LOPC Likelihood	Direct ignition Successful	Fire & Gas Detection Successful	protection system Successful	Ultimate Incident Outcome	Event Combinations	Ultimate Incident Frequency	Event Description
LOPC frequency 7,52E-06	Direct ignition 0,7 (Yes)	0,985	0,99021	Jet Fire	ABCD	5,14E-06	Frequency of direct ignition given Fire and Gas system and Protection system availability
			0,00979	Jet Fire	ABCd	5,08E-08	Frequency of direct ignition given Fire and Gas system availability and Protection system unavailability
		0,015	0,99021	Jet Fire	ABcD	7,73E-10	Frequency of direct ignition given Fire and Gas system unavalibility and Protection system availability
			0,00979	Jet Fire	ABcd	7,73E-10	Frequency of direct ignition given Fire and Gas system and Protection system unavalibility
	Delayed ignition 0,3 (No)	0,985		Harmless	AbC	2,22E-06	Frequency of Harmless release given fire and gas detection system successes to detect the leak
		0,015	0,99021	UNVCE	AbcD	3,35E-08	Frequency of UNVCE given presence of delayed ignition source and fire and gas detection system fails to detect the leak and protection system success
			0,00979	UNVCE	Abcd	3,31E-10	Frequency of UNVCE given presence of delayed ignition source and fire and gas detection system fails to detect the leak and protection system failure
				Jet fire Frequency		5,189E-06	
				UNVCE Frequency		3,386E-08	
				Harmless Frequency		2,223E-06	
					Total	7,446E-06	

Figure 11`: "Slug catcher LOPC" ETD Assuming Design Initiating Events

A	B	C	D				
Initiating LOPC Likelihood	Direct ignition Successful	Fire & Gas Detection Successful	protection system Successful	Ultimate Incident Outcome	Event Combinations	Ultimate Incident Frequency	Event Description
LOPC frequency 4,20E-05	Direct ignition 0,7 (Yes)	0,985	0,99021	Jet Fire	ABCD	2,86E-05	Frequency of direct ignition given Fire and Gas system and Protection system availability
			0,00979	Jet Fire	ABCd	2,83E-07	Frequency of direct ignition given Fire and Gas system availability and Protection system unavailability
		0,015	0,99021	Jet Fire	ABcD	4,31E-09	Frequency of direct ignition given Fire and Gas system unavalibility and Protection system availability
			0,00979	Jet Fire	ABcd	4,31E-09	Frequency of direct ignition given Fire and Gas system and Protection system unavalibility
	Delayed ignition 0,3 (No)	0,985		Harmless	AbC	1,24E-05	Frequency of Harmless release given fire and gas detection system successes to detect the leak
		0,015	0,99021	UNVCE	AbcD	1,87E-07	Frequency of UNVCE given presence of delayed ignition source and fire and gas detection system fails to detect the leak and protection system success
			0,00979	UNVCE	Abcd	1,85E-09	Frequency of UNVCE given presence of delayed ignition source and fire and gas detection system fails to detect the leak and protection system failure
					Jet fire Frequency	**2,893E-05**	
					UNVCE Frequency	**1,888E-07**	
					Harmless Frequency	**1,240E-05**	
					Total	**4,152E-05**	

Figure 12: “Slug catcher LOPC” ETD Assuming Updated Initiating Event

A	B	C	D				
Initiating LOPC Likelihood	Direct ignition Successful	Fire & Gas Detection Successful	protection system Successful	Ultimate Incident Outcome	Event Combinations	Ultimate Incident Frequency	Event Description
LOPC frequency 2,04E-06	Direct ignition 0,7 (Yes)	0,985	0,99021	Jet Fire	ABCD	1,39E-06	Frequency of direct ignition given Fire and Gas system and Protection system availability
			0,00979	Jet Fire	ABCd	1,37E-08	Frequency of direct ignition given Fire and Gas system availability and Protection system unavailability
		0,015	0,99021	Jet Fire	ABcD	2,09E-10	Frequency of direct ignition given Fire and Gas system unavalibility and Protection system availability
			0,00979	Jet Fire	ABcd	2,09E-10	Frequency of direct ignition given Fire and Gas system and Protection system unavalibility
	Delayed ignition 0,3 (No)	0,985		Harmless	AbC	6,01E-07	Frequency of Harmless release given fire and gas detection system successes to detect the leak
		0,015	0,99021	UNVCE	AbcD	9,07E-09	Frequency of UNVCE given presence of delayed ignition source and fire and gas detection system fails to detect the leak and protection system success
			0,00979	UNVCE	Abcd	8,97E-11	Frequency of UNVCE given presence of delayed ignition source and fire and gas detection system fails to detect the leak and protection system failure
					Jet fire Frequency	**1,404E-06**	
					UNVCE Frequency	**9,158E-09**	
					Harmless Frequency	**6,014E-07**	
					Total	**2,014E-06**	

Figure 13: "Coils LOPC" ETD Assuming Design Initiating Event

Note: Delayed ignition scenario only occur at start up.

A	B	C	D				
Initiating LOPC Likelihood	Direct ignition Successful	Fire & Gas Detection Successful	protection system Successful	Ultimate Incident Outcome	Event Combinations	Ultimate Incident Frequency	Event Description
LOPC frequency 8,39E-06	Direct ignition 0,7 (Yes)	0,985	0,99021	Jet Fire	ABCD	5,73E-06	Frequency of direct ignition given Fire and Gas system and Protection system availability
			0,00979	Jet Fire	ABCd	5,66E-08	Frequency of direct ignition given Fire and Gas system avalibility and Protection system unavailability
		0,015	0,99021	Jet Fire	ABcD	8,62E-10	Frequency of direct ignition given Fire and Gas system unavalibility and Protection system availability
			0,00979	Jet Fire	ABcd	8,62E-10	Frequency of direct ignition given Fire and Gas system and Protection system unavalibility
	Delayed ignition 0,3 (No)	0,985		Harmless	AbC	2,48E-06	Frequency of Harmless release given fire and gas detection system successes to detect the leak
		0,015	0,99021	UNVCE	AbcD	3,74E-08	Frequency of UNVCE given presence of delayed ignition source and fire and gas detection system fails to detect the leak and protection system success
			0,00979	UNVCE	Abcd	3,70E-10	Frequency of UNVCE given presence of delayed ignition source and fire and gas detection system fails to detect the leak and protection system failure
				Jet fire Frequency		5,785E-06	
				UNVCE Frequency		3,774E-08	
				Harmless Frequency		2,479E-06	
					Total	8,301E-06	

Figure 14: “Coils LOPC” ETD Assuming Updated Initiating Event

Note: Delayed ignition scenario only occur at start up.

Table 5: Individual Risk Tolerability Criteria (DNVGL, 2015)

Risk Level	Individual Risk (per year) -Workers	Individual Risk (per year) - Public
Intolerable	> 1 × 10-3	> 1 × 10-4
Tolerable if ALARP	≥ 1 × 10-6 and ≤ 1 × 10-3	≥ 1 × 10-6 and ≤ 1 × 10-4
Broadly Acceptable	< 1 × 10-6	

Table 6: Calculation of IR and PLL of the accidental scenarios understudy

Scenario	F_C (per year)	PLL (per year)	LSIR (per year)	IRPA (per year)
	$D.\left(\prod_{j=1}^{J} PFD_{i,j}\right)$	$PLL = F_C.N_F$	$LSIR = F_C.P_{fatality}$	$F_C.P_{fatality}.P_{present}$
Failure of slug catcher (N = 78 and NF= 1,44)[2]				
QRA Study[1] (ADVANTICA, 2008)	3,17E-04	4,56E-04	3,23E-06	8,08E-07
Complying with MIT intervals	5,19E-06	7,47E-06	5,19E-08	1,30E-08
Deferral of MIT	2,89E-05	4,17E-05	2,89E-07	7,23E-08
Failure of Heater Coils (N = 17 and NF = 1,78)[2]				
QRA Study	1,02E-05	1,82E-05	6,30E-07	1,58E-07
Complying with MIT intervals	1,40E-06	2,50E-06	1,40E-07	3,51E-08
Deferral of MIT	5,79E-06	1,03E-05	5,79E-07	1,45E-07

Notes: 1. Frequency of consequences (Fc) is calculated reference to equation 4

2. Reference to QRA study report (ADVANTICA, 2008)

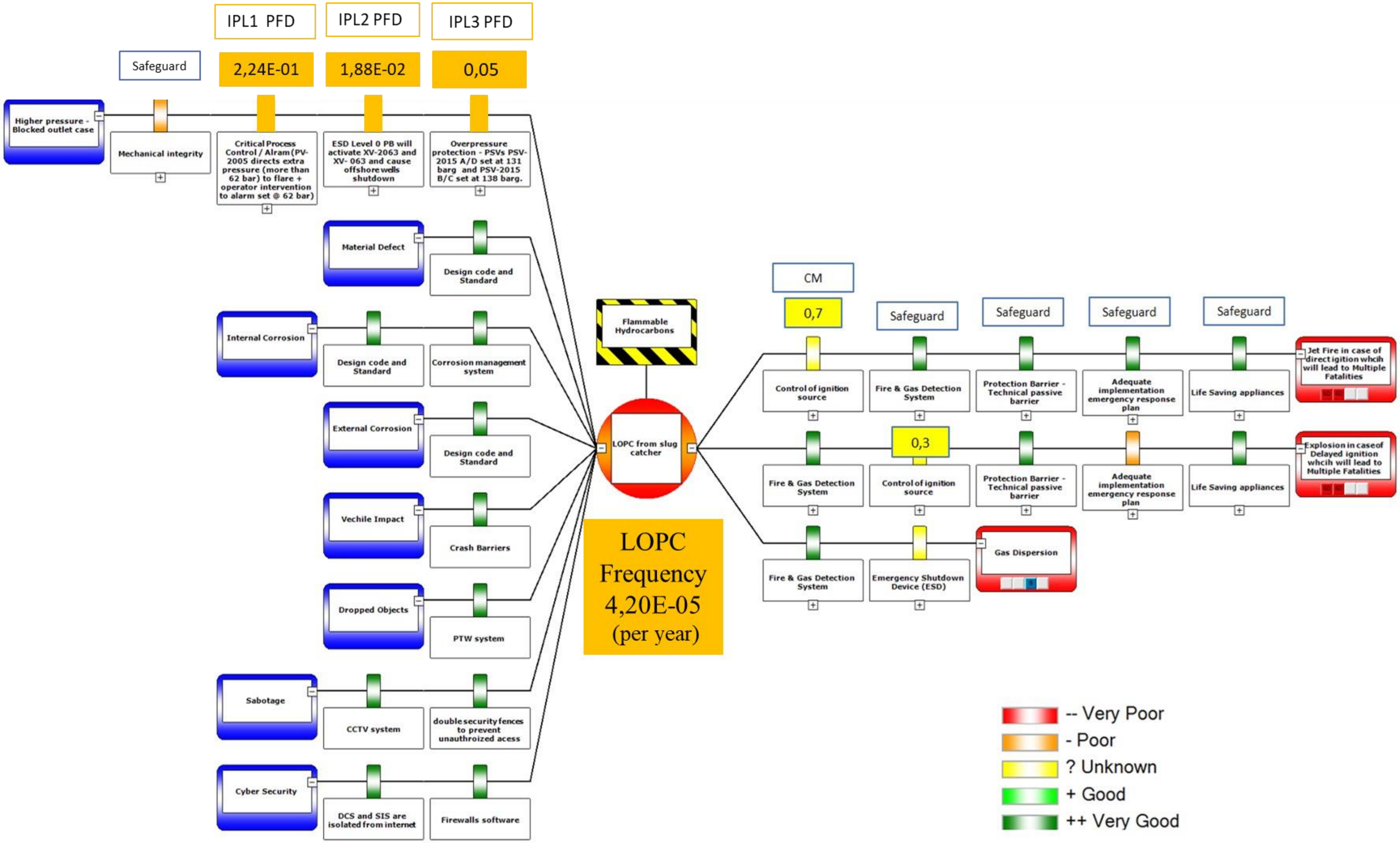

Figure 15 Quantified BTD of slug catcher LOPC case

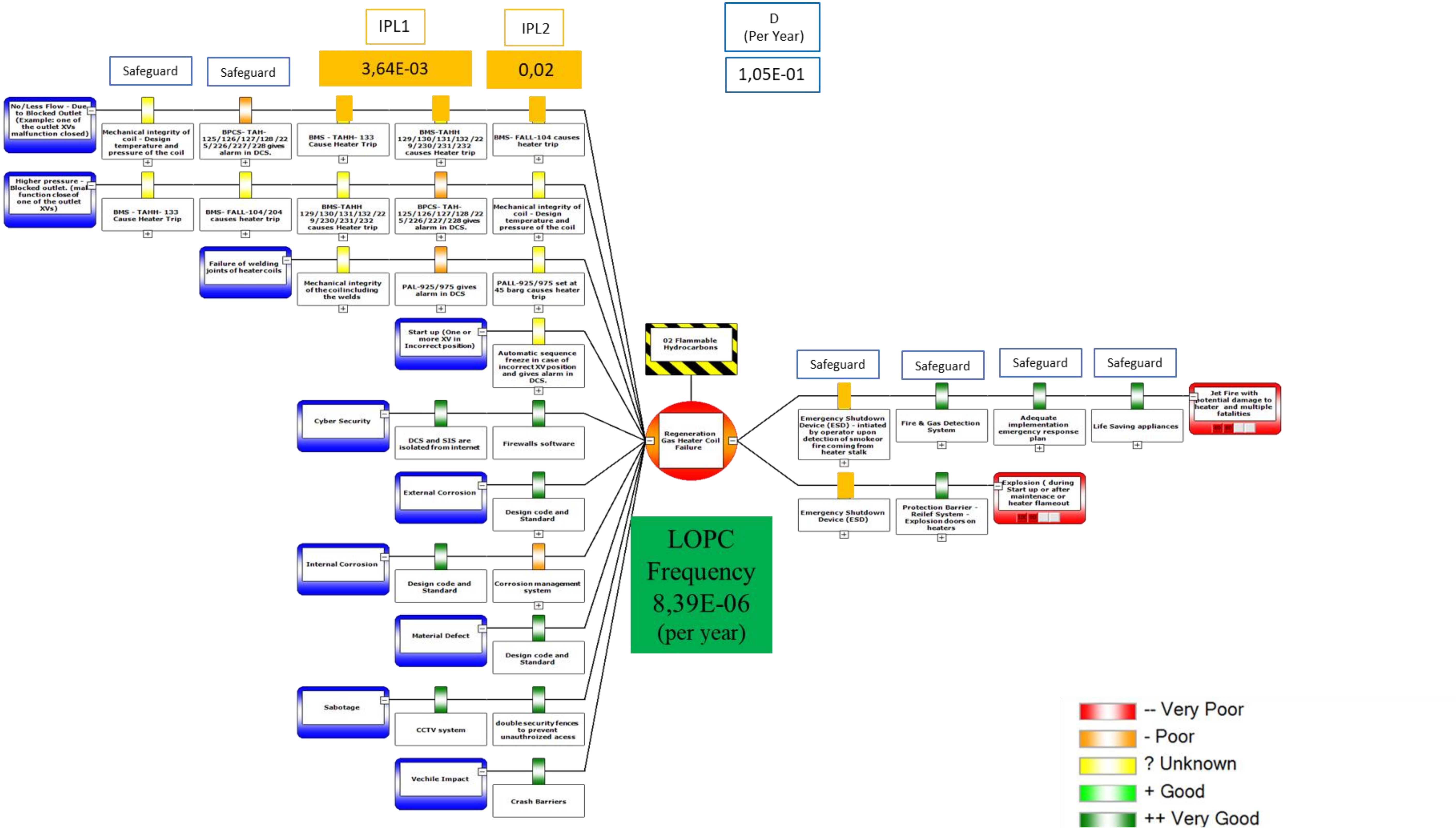

Figure 16 Quantified BTD of regeneration gas heater LOPC case

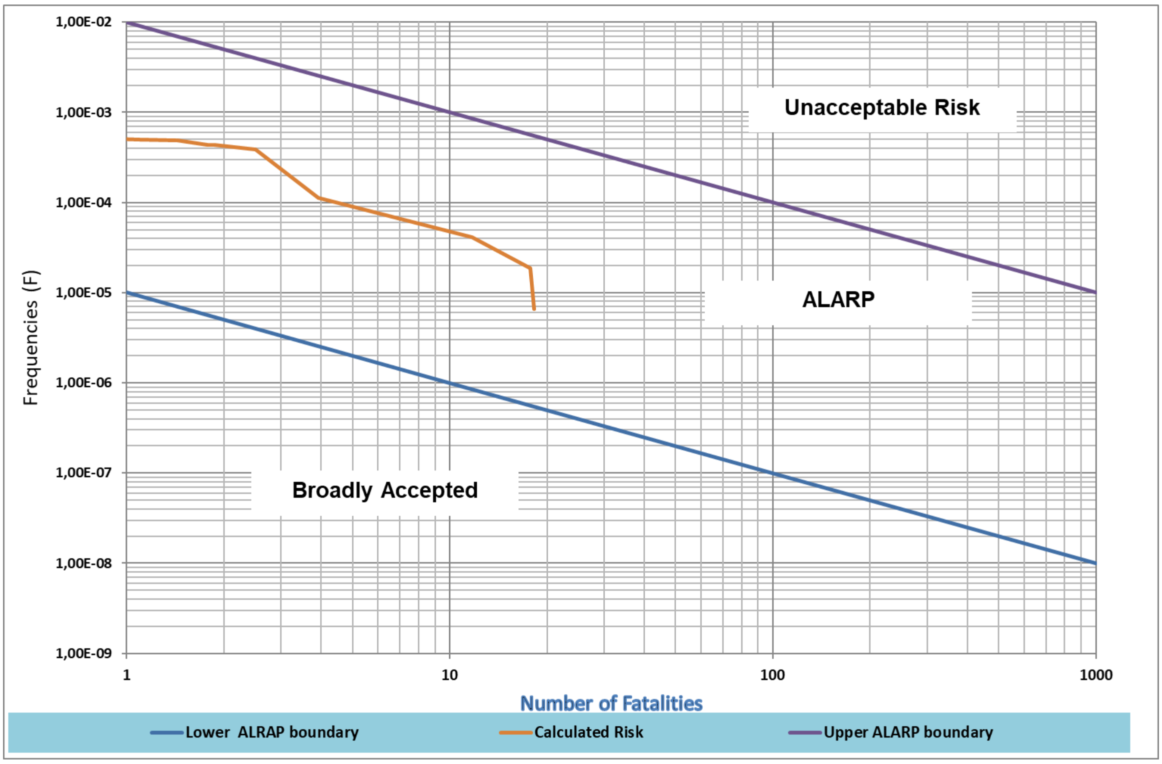

Figure 17 : Design FN-Curve of the Case Study (ADVANTICA, 2008)

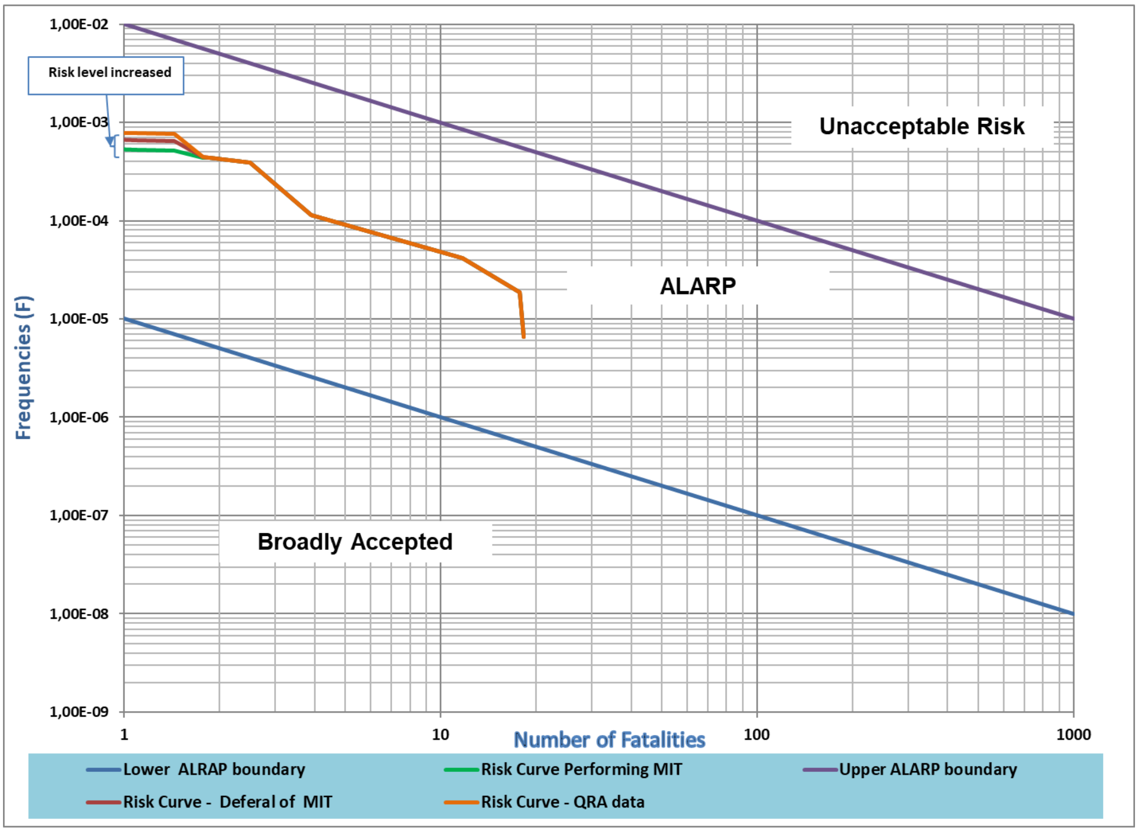

Figure 18: Operational FN Curve

About the Author

Has more than 20 years' experience in Oil & Gas industry mainly in operational sites. Participated in process safety engineering studies. Has extensive experience in implementing risk-based management systems. Has a Master of Science in Engineering (MSC(ENG)) in Process Safety and Loss Prevention (PSLP) from Sheffield University and Master of science (M.Sc.) in environmental physics specialized in Quantitative Risk Assessment (QRA) and risk management from Institute of Graduate Studies and Research (IGSR) Alexandria University. A Certified Energy Manager (CEM) from Association of Energy Engineers and a Functional safety engineer (TÜV Rheinland) (SIS & PH & RA).

References

ADVANTICA. 2008. *Case study Quantitiave Risk Assessemnet study.* 2008.
API. 2000. *API 581, Risk-Based Inspection.* 2000.
Ball, D. J. and Floyd, Peter. J. 1998. *Societal Risks- Final Report.* 1998.
BG. 2012. *Operational Risk Assessment Standard.* 2012.
Blacklaw, Alan, Ward, Al and Cassidy, Kevin. 2011. *The Cumulative Risk Assessment Barrier Model.* Aberdeen : the SPE Offshore Europe Oil and Gas Conference and Exhibition held in Aberdeen, UK, 6–8 September 2011, 2011.
CCPS. 2000. *Guidelines for Chemical Process Quantitative Risk Analysis (CPQRA).* s.l. : Center for Chemical Process Safety/AIChE, 2000.
—. 2009. *Guidelines for Developing Quantitative Safety Risk Criteria.* s.l. : Center for Chemical Process Safety /AICHE, 2009.
—. 2001. *Layer of Protection Analysis SIMPLIFIED PROCESS RISK ASSESSMENT.* New York, New York 10016-5991 : Center for Chemical Process Safety, 2001. ISBN 0-8169-0811-7.
DNVGL. 2015. Case study *SIL detemirnation study.* 2015.
—. 2015. *Caser study HAZOP study.* 2015.
—. 2015. *Case study Safety case.* 2015.
Franks, Andrew. 2005. *Lines of Defence/Layers of Protection Analysis in the COMAH Context.* s.l. : Amey VECTRA Limited for the Health and Safety Executive of UK, 2005.
HaSPA. 2012. *The Core Body of Knowledge for.* Health and Safety Professionals Alliance. Tullamarine, Victoria, Australia : Safety Institute of Australia Ltd,, 2012. ISBN 978-0-9808743-1-0.
Hausand, Marvin and Hoyland, Arnljot. 2004. *System Reliability Theory Models, Statistical Methods,and Applications.* s.l. : Wiley, 2004.
I.L. Hirst, D.A. Carter. 2002. *"worst case" methodology for obtaining a rough but rapid indication of the societal risk from a major accident hazard installation.* s.l. : ELSEIVER, 2002. pp. 223–237.
IChemE. 2009. An independent review of HSE methodology. s.l. : Crown, 2009.
IEC. 2003. Functional safety – Safety instrumented systems for the process industry sector - Part 3 Guidance for the determination of the required. s.l. : International Electrotechnical Commission, 2003. IEC 61511-3:2003(E).
J.K.Vrijling and Gelder, P.H.A.J.M. van. 1997. *SOCIETAL RISK AND THE CONCEPT OF RISK AVERSION.* Stevinweg, Netherlands : Department of Civil Engineering, Delft University of Technology, 1997.
Mehmood, Ahmad and Marco, Pontiggia. 2015. *Modified Swiss Cheese Model to Analyse the Accidents.* 2015. ISBN 978-88-95608-34-1;.
Pitblado, R., et al. 2016. *Concepts for dynamic barrier management.* 2016. pp. 741-746.
Sklet, Snorre and Hauge, Stein. 2015. *Safety barriers to prevent release of hydrocarbons during production of oil and gas.* s.l. : SINTEF Industrial Management, 2015.
Stein, Hauge and Knut, Øien. 2016. *Guidance for barrier management in the petroleum industry.* s.l. : SINTEF Technology and Society, 2016.