Applying Process Safety Experiences and Lessons Learnt to Achieve Improvements In Plant Up-Time and Stability of Production

Anees I Ansari, Mohammad Moonis, Mazhar Sheikh

Consultants, Pleiades Global Limited (PGL), Portsmouth, United Kingdom

Abstract: Application of process safety reviews and principles for identifying major process hazards, their potential consequences, required risk reduction or process control measures is widely and popularly used across all sectors. Since its inception as a discipline, process safety has made commendable contribution to minimize harm to the people, environment or assets.

However, it has been frequently observed that the plant design always has some room for rationalization of protection and control systems. This can be owed to several factors such as poor initial design, changes in process parameters over time or may be that a holistic plant wide study could never be carried out. The importance of adequately protected process facility cannot be stressed enough. However, irrespective of the organization, an overly protected design will lead to unwanted trips and therefore loss of production and revenue without providing enhancement to safety.

This paper presents insights gained through experience and realization that rationalising process safety and process control design in existing plants may lead to increased plant up-time and production stability, without compromising on safety. Process assessments and cost benefit analysis based methodologies were used to demonstrate objectively that even for facilities with very low production rates, implementing additional process control proves to be very good value. The methodology also provides an objective basis to develop a case for downgrading an exiting safety or control measure.

Examples have been developed based on typical hydrocarbon fuel processes and cover generic but most common issues such as single point failures, cascade effects, safety instrumented function rationalisation, common equipment, emergency power loads and testing or maintenance of safety critical systems are also discussed. The paper also touches upon key points to consider in training of field maintenance personnel to address common pitfalls during maintenance e,g, during testing and calibration of fire and gas detectors.

Keywords: Process hazard analysis, PHA, HAZOP, process safety, process control, operations, uptime, down-time, SCE, production deferment, cost benefit analysis, CBA

Context

Process safety reviews such as HAZOPs and SIL evaluations are well-established methodologies for safety reviews. However, HAZOPs are widely used for assessing deviations from the design intent and typically, the output is recommending some kind of protection measures such as process control or procedures. However, one limitation of HAZOPs is that it assesses one failure at a time rather than assessing the design from the perspective of how the whole design together may impact operational ease / difficulty. Similarly a SIL assessment (e.g. LOPA) is mostly used to recommend ratings for process control loops to avoid a hazard.

Nonetheless, once a plant has been operational for sometime and some operational experience, lessons, trends, bottleneck or issues have been recorded, a holistic plant-wide rationalisation study, based on operational issues may be very beneficial. The aim of such a rationalization study is not to compromise safety in any way but to review known problem areas, identifying potential bad actors and analyzing them further. The output of such a study may be improving an existing safety system or even removing it. However, it goes without saying, that there may be reluctance to put in more safety control measures / devices because of operational or budgetary reasons. It has been duly observed that once a risk reduction measure has been ‘designed in’, there may be reluctance to take it out unless very strong evidence can be produced in support. Such issues may be more prominent in bigger or more bureaucratic set-ups such as National Oil Companies or geographical regions where process safety is still an evolving discipline.

This paper present a methodology which can be used to provide objective evidence, based upon ease of operations and production outputs, to support the recommendations regarding improving or altering an existing safety or control measure. Such objective evidence can prove very useful in developing a business or management case for a recommended change.

This paper is based on our experiences gained through various studies and reviews such as:

- Chairing of and participating in Process Hazard Assessments (PHAs) and Management of Change (MoC) reviews;
- Identification of gaps in process safety rationalization in PHAs or MoCs; and
- Carrying out specific process safety rationalization or re-validation studies

The analysis is based on experience gained and reviews carried out across varied geographical regions, safety cultures and regulatory frameworks. It should however be noted that rationalization of plant design is a very wide topic. Methodology for carrying out such a review may be very different from one plant to another. Careful planning and review will be required before carrying out rationalization of process safety of a process plant. The intention here is to present the observations and discussions generically using from common aspects of plant design, operation and maintenance. The expectation is that the principles of methodologies presented here can be easily applied to any study aimed to achieve similar results.

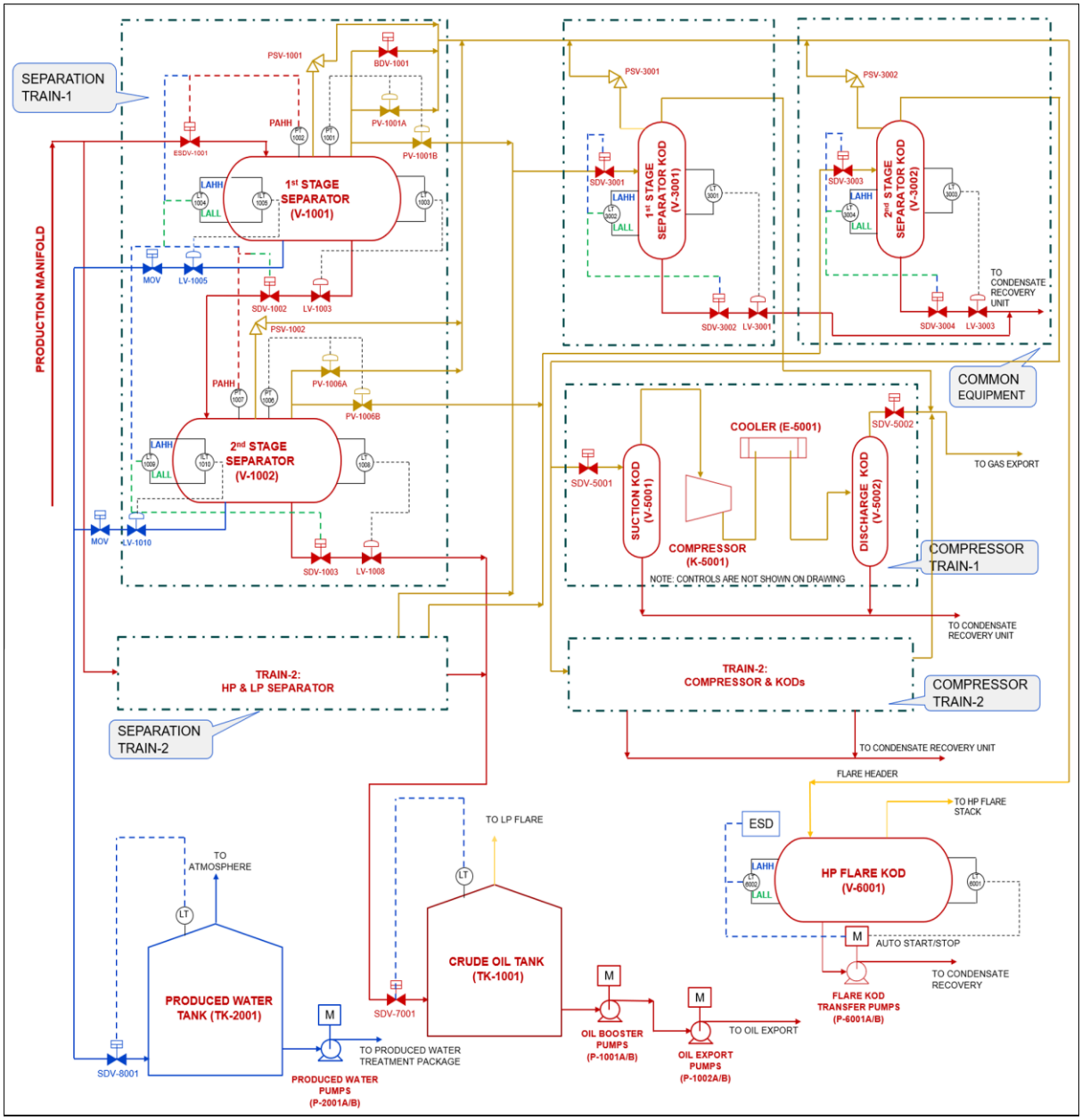
Introduction

A generic process set-up, based on typical hydrocarbon processing facilities was developed for the purposes of this paper. The aim is to share the experiences and insights gained through real situations and reviews in an anonymous and generic way. The users or any third parties hired for carrying out similar studies can apply the insights and methodology to specific cases. This process is schematically shown in Figure 1 and comprises of two trains. Figure 1 shows train-1 in detail, while schematic blocks are used to represent train-2 equipment. The associated process controls and shutdown loop(s) for each equipment are also shown.

Each train has independent 1st Stage and 2nd stage separation and gas compression processes. The 1st stage and 2nd stage Separator KODs are common equipment shared between the two trains. The other equipment shared between the two trains are HP Flare KOD (V-6001), Produced Water Tank (TK-2001) and Crude Oil Tank (TK-1001). The two trains are assumed to be in duty/standby set-up.

This example process is used in this paper for describing some simple yet commonly occurring scenarios, which may impact plant uptime.

Figure 1: Schematic Showing a Generic Crude Oil Separation and Export Process



Process Description

Well fluids from various fields are received at a common production manifold from where the well fluids are routed production facility presented in Figure 1. At the production facility, the fluids are separated into Oil, Gas and Water streams at the 1st Stage Separator (V-1001).

Gas stream separated in the 1st stage separation step is sent to the gas export directly while the oil stream with associated gas is channeled to the LP Separation (V-1002). The gases separated at the 1st and 2nd Stage 2 separation, are routed to common 1st and 2nd Stage Separator KODs (V-3001 and V-3002), respectively. Gases from the V-3001 are then sent for gas compression train(s) prior to gas export. *Note: Separator KODs are normally provided as an intermediary step where the separation and compressor trains are not very close to each other*.

HP Flare KOD (V-6001) is provided, where any off-gas will be routed to in case of any emergency or operational upset.

Oil stream from the 2nd stage separation is routed to the crude oil tank TK-1001 and then exported through the export pumps (main and booster). Similarly, Produced Water (PW) is routed to the produced water treatment units via PW Tank TK-1002.

Process parameters for the process are provided in Table 1.

Table 1: Process Parameters

Equipment	Pressure (Operating / Design), barg	Temperature (Operating / Design), degC	Remarks
1st Stage Separator (V-1001)	20/27	37/86	-
2nd Stage Separator (V-1002	4.8/20	37/67	-
1st Stage Separator KOD (V-3001)	19.5/27	37/86	-
2nd Stage Separator KOD (V-3002)	4.5/20	37/67	-
Compressor Trains	19.5/27	37/86	Not on emergency load
PCV-1001A	20/27	37/86	Not designed for full blocked outlet
PSV-1001	27	-	Full blocked outlet case/fire case
PCV-1006A	4.8/20	37/67	Not designed for full blocked outlet
PSV-1002	20	-	Full blocked outlet case/fire case
HP Flare KOD (V-6001)	1.5/5	27/86	-
Oil Booster Pumps (P-1001A/B)	4.5/12	30/90	Provided with emergency power
Oil Export Pumps (P-1002A/B)	25/35	35/90	Provided with emergency power
Produced Water Pumps (P-2001A/B)	7/12	27/86	Not on emergency load
Trains 1 and 2 are in duty / standby set-up.			

The following Emergency Shutdown (ESD) hierarchy has been adopted for the process:

Level-1 Shutdown: ESD-1 actuation leading to plant shutdown with depressurization including Blowdown.

Level-2 Shutdown: ESD-2 actuation leading to plant shutdown without depressurization.

Level-3 Shutdown: ESD-3 actuation leading to respective train shutdown without depressurization.

Level-4 Shutdown: ESD-4 actuation leading to respective equipment shutdown without depressurization.

Methodology

The first step in any plant design rationalization evaluation is a thorough design review. The design review shall look into plant history and trends for any known bad actors causing operational upsets. One the bad actors are identified, these may be assessed ahead of reviewing rest of the plant. A quick and simple way to perform review may involve considering each process stream on the facility PFD and referring to the detailed P&IDs later. Each process stream shall be followed through, in sequence, for the potential bottlenecks.

For the purpose of methodology explained in this paper, six representative scenarios were shortlisted. These scenarios are based on plant design, operation and maintenance and represent some of the most common causes of plant downtime or production deferment. The scenarios are based on the process depicted in Figure 1 and are listed below:

1. Triggers for single point failures resulting in immediate plant shutdown;
2. Cascaded effects of single point failure in an area or equipment;
3. Rationalisation of non SIL rated SIFs;
4. Production critical items not provided with emergency power provisions.
5. Common equipment shared between identical trains; and
6. Operator error during maintenance or testing of critical elements e.g. fire and gas detection, leading to Level-1 shutdown.

General methodology adopted is carrying out assessment of design or known issues, identifying modes of failure, steps and time required to re-start and recommending control measure to prevent the unwanted impact(s). Where, added control measures are recommended, these then shall be subject to a cost benefit analyses. The main terms used in the discussion along with relevant assumptions and data are provided under the subsequent sub-heading below:

Scenario Description: Description of a particular test case(s) developed for each of the six scenarios listed above.

Source Elements: The equipment and / or conditions triggering a shutdown condition for each scenario. This can be a transmitter, F&G detector, effect of another abnormal situation etc.

Failure modes: Different ways, along with the contributory steps, how an abnormal situation may lead to a shutdown.

Actions and time required to re-start: remedial actions required to re-start the facility and time required for each step. The representative times used in the analyses are presented in Table 2 to Table 4 below:

Table 2: Total Representative Time Required for Plant Start-up

Sr. No.	Tag No.	Position Before Shutdown	Position After Shutdown	Field Reset (Yes/No)	Start from DCS (Yes/No)	Time req to Restart (s)
Area: Separator						
1	ESDV-1001	OPEN	CLOSE	Yes	No	600
2	SDV-1002	OPEN	CLOSE	Yes	No	600
3	SDV-1003	OPEN	CLOSE	Yes	No	600
4	SDV-3001	OPEN	CLOSE	Yes	No	600
4	SDV-3002	OPEN	CLOSE	Yes	No	600
4	SDV-3003	OPEN	CLOSE	Yes	No	600
5	SDV-3004	OPEN	CLOSE	Yes	No	600
Area: Compressors						
1	SDV-5001	OPEN	CLOSE	Yes	No	600
2	SDV-5002	OPEN	CLOSE	Yes	No	600
1	K-5001	RUNNING	STOP	Yes	No	1800
1	P-1001A/B	RUNNING	STOP	Yes	No	600
1	P-1002A/B	RUNNING	STOP	Yes	No	600
2	P-2001A/B	RUNNING	STOP	Yes	No	600
Representative total time required for plant start-up						**9000**

Table 3: Total Representative time required for re-instating normal operations following ESD-1

Action Initiated	Time Required in seconds and (minutes)
Time required to plant Shutdown with depressurization	1800 (30)
Decision making to restart the plant	3600 (60)
Plant System Pressurization	3600 (60)
Time required for plant start-up (Table 1)	9000 (150)
Total time taken for plant back to Normal operation	**5 hours**

Table 4: Total Representative time required for re-instating normal operations following ESD-2

Action Initiated	Time Required in seconds and (minutes)
Time required to plant Shutdown	900 (15)
Decision making to restart the plant	1800 (30)
Time required for plant start-up (Table 1)	9000 (150)
Total time taken for plant back to Normal operation	**3 hours**

Deferred production cost: Having assessed the total time to restart, deferred production volume can be calculated. in some cases, it may be argued that deferred production is not the 'lost production'. However, deferred production does have some cost implications. This may be due to factors such as an operator's contractual duties to end-users, cash flow requirements,

or to satisfy the projects' Internal Rate of Return (IRR)' requirements. Potential project IRR has been selected as a factor for working out money lost as a fraction of deferred production in the assessment presented here. Depending upon the geographical regions / operating costs the project's costs may vary widely. Therefore, IRR values of 25% and 75% have been chosen in the assessment to present varied sensitivities to the analyses.

This is calculated using the following formula:
Deferred production value (USD year^{-1}) = Daily production (barrels day^{-1}).(365days).(IRR).Price of BOE (USD barrel^{-1})

Cost benefit analysis: Any recommendations raised for the above scenarios, may be subjected to a screening for implementation, based on Cost Benefit Analyses (CBA). The methodology involves comparing the 'cost of implementing a recommendation', against the benefit obtained which, on our case is avoiding the monetary value of the deferred production.

The essence of CBA is that the cost of implementing a recommendation shall not be too high compared to the benefit obtained. Values of 'Disproportionation Factor (DF)' between 1 and 10 are generally taken as acceptable to implement a risk control measure, where fatalities are involved (HSE, UK[1]). As we have mainly dealt with financial losses (instead of people safety or major accident hazard) in our assessment, we have chosen the cost benefit ratio at a lower value of 2, as the criteria for adopting any recommendations proposed to improve the plant uptime. An important factor to consider here is the time in service factor – which is the cost of risk control measure distributed over the expected plant or instrument life.

Therefore, assuming a 10-year usable life, the actual cost / benefit ratio for the scenarios considered our assessment can be calculated as:

$$\text{Cost Benefit Ratio} = \frac{\text{(Cost of implementing a plant uptime recommendation / 10 years)}}{\text{Total deferred production avoided per year}}$$

The cost of implementing a recommendation is based on realistic equipment values as far as possible in our assessments. The final values used in the analyses include procurement, administrative and installation considerations. However, the maintenance costs or depreciation over the life of equipment are not included.

Example implementation of the methodology

This section presents implementation of the subject methodology for each of the representative scenarios described in the previous section.

Scenario 1: Triggers for single point failures resulting in immediate plant shutdown;

This scenario considers that the level transmitter LIT-6002 on the HP Flare KOD (V-6001), malfunctions and initiates an unintended Level-2 shutdown. The level-2 shutdown will cause closure of all the ESDVs across the plant and other equipment such as pumps, compressors, heaters etc. leading to deferment of production. Re-starting the plant will involve several steps, each of which will contribute to the time required to re-start. Re-starting may be more onerous when it involves facilities spread over a bigger area or a larger sequence of operations as per the plant manual. These steps, along with the estimates of time required for implementing them, are provided in Table 4 (ESD-2). A recommendation to avoid this scenario may be to provide additional Level Transmitters with LT-6002 with 2oo3 logic.

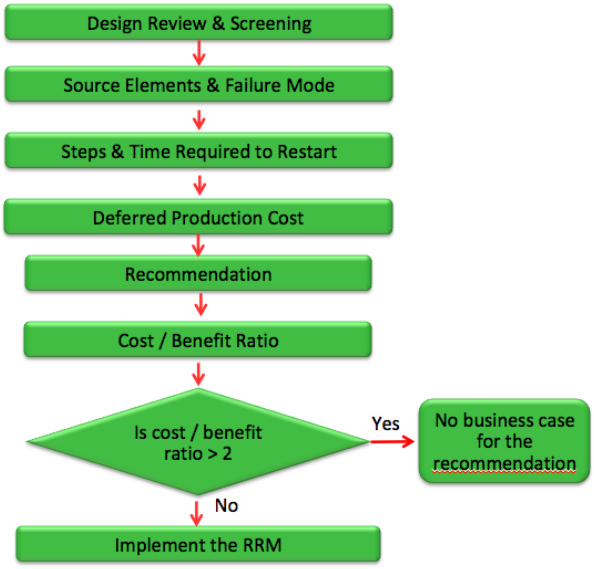
Having evaluated these steps and therefore, the time required to re-start, the value of deferred production can be calculated. Then, as described in the previous section, a monetary value based on two different IRRs can be calculated. The cost of implementing the recommendation can then be compared against the potential value of deferred production to estimate the cost-benefit ratio. This assessment is presented in Table 5 and the methodology is schematically presented in Figure 2.

As can be seen in Table 5, even for very low daily production rates, the calculated DF is much lower than the selected criteria of cost benefit ratio <2 for adopting the recommendation.

Table 5: Evaluation of Scenario 1

Equipment	Source Element	Failure Mode	Frequency of occurrence per year, (F)	Sequence of Events	Expected duration of plant outage (hrs)	Total planned production (BBLs) per day	Total Deferred production Loss (USD) 60 USD/BBL per year	Recommendations	Potential total cost of implementing the RRM (USD)	Per year cost of implememting the RRM (plant life = 10 years) (USD)	Cost to Benefit Ratio (CBA)	Implement the RRM (Y/N)
(25% IRR)												
HP Flare KOD (V-6001)	LT-6002	Malfunction of LT-6002 showing level high but actual level is normal	0.1	Leading to Level 2 shutdown (ESD-2)	3	5000	938	Provide additional LT-6002 with voting logic 2oo3 to avoid spurious trip.	8000	800	0.85	YES
(75% IRR)												
HP Flare KOD (V-6001)	LT-6002	Malfunction of LT-6002 showing level high but actual level is normal	0.1	Leading to Level 2 shutdown (ESD-2)	3	5000	2813	Provide additional LT-6002 with voting logic 2oo3 to avoid spurious trip.	8000	800	0.28	YES

Figure 2: Methodology for Evaluating Scenario 1



Scenario 2: Cascaded effects of single point failure in an area or equipment

Again referring to the schematic provided in figure 1, we assume LT-3004 on 2nd Stage Separator KOD (V-3002) causing a spurious high-high level trip during normal operations and initiating closure of SDV-3003 on inlet of the 2nd Stage Separator KOD (V-3002). This will lead to compressors (both the trains will be impacted) not receiving any feed from V-3002 and therefore going into shutdown following low suction pressure.

Also, it is assumed that this separator KOD and the 1st and 2nd stage separators will be at 'normal liquid level' when the spurious trip occurs; on the upstream side, the following sequence of events will potentially occur:

1) If the PCV (PV-1006A) is designed for blocked outlet case, then the gas will safely be discharged to flare. The only consequence in this case will be loss of gas, also leading to environmental issues.

2) However, as in our process, this PCV (PV-1006A) is not designed (Refer Table 1) for the blocked outlet case, the following sequence of events will take place:

   a. Overpressurisation of the 2nd Stage Separation, up to the High-High Pressure trip set point (PT-1007).

   b. PAHH-1007 will close SDV-1002, at the 1st stage separator outlet.

   c. This will cause liquid level built-up in the 1st Stage Separator (V-1001), eventually leading to LAHH-1004 to act to close ESDV-1001 at the inlet.

d. The 2nd Stage Separator will stop receiving feed. The level in this separator will eventually stabilize as per the process control provided and level and pressure control valves turning 'closed'.

As mentioned in Table 1, for our assessment we have assumed duty-standby configuration for the two trains. Therefore, closure of ESDV-1001 will lead to deferment of entire production. However, even if the two trains were running as parallel, this scenario would have caused deferment of the entire production, as the source element is equipment shared between the two trains.

A recommendation to avoid this scenario will be to provide additional Level Transmitters with LT-3004 with 2oo3 logic.

Similar to the discussion presented under scenario 1, a CBA was carried out for this scenario and is presented in Table 6. It can be seen in Table 6 that even for very low daily production rates, the calculated cost benefit ratio is much lower than the selected criteria of <2 for adopting the proposed recommendation.

Table 6: Evaluation of Scenario 2

Equipment	Source Element	Failure Mode	Frequency of occurrence per year, (F)	Sequence of Events	Expected duration of plant outage (hrs)	Total planned production (BBLs) per day	Total Deferred production Loss (USD) 60 USD/BBL per year	Recommendations	Potential total cost of implementing the RRM (USD)	Per year cost of implememting the RRM (plant life = 10 years) (USD)	Disproportionation factor (CBA)	Implement the RRM (Y/N)
(25% IRR)												
2nd Stage Separator KOD (V-3002)	LT-3004	Malfunction of LT-3004 showing level high but actual level is normal	0.1	Leading to Level 2 shutdown (ESD-2)	3	5000	938	Provide additional LT-3004 with voting logic 2oo3 to avoid spurious trip.	8000	800	0.85	YES
(75% IRR)												
2nd Stage Separator KOD (V-3002)	LT-3004	Malfunction of LT-3004 showing level high but actual level is normal	0.1	Leading to Level 2 shutdown (ESD-2)	3	5000	2813	Provide additional LT-3004 with voting logic 2oo3 to avoid spurious trip.	8000	800	0.28	YES

Scenario 3: Rationalisation of non SIL Rated SIFs

As per Table 1 (and common engineering practice), design pressure of 2nd Stage Separator (V-1002) is equal to the maximum operating pressure of the 1st Stage separator. Therefore, it can be safely assumed that SIL rating for the SIF loop LT-1004, provided on the first stage separator outlet would have been assessed as SIL 0. Note that, in reality this information shall be referenced from plant's SIL classification study.

As per IEC 61511-3 (IEC, 2016), no special safety requirements are to be implemented if a SIF loop is classified as non SIL rated. This may lead to use of lower reliability components in such loops. The assessment(s) covered scenarios where such loops were leading to shutdowns, whereas only an alarm function could have been adequate.

For this assessment, we assume LT-1004 causing a spurious low-low level trip during normal operations. Also, it is assumed that 1st Stage Separator will be at 'normal liquid level' when the spurious trip occurs. This will lead to the closure of SDV-1002 on the outlet of V-1001, which, in turn will lead to the following sequence of events:

1) Liquid build-up in the 1st Stage Separation, up to the High-High level trip set point.

2) The 2nd Stage Separator will stop receiving feed. The level in this separator will eventually stabilize as per the process control provided and level and pressure control valves turning 'closed'.

3) This will lead to compressor not receiving any feed from train 1 and therefore going into shutdown following low suction pressure. This implies that 100% production will be impacted if the trains are configured as duty-standby. If the train configuration is 2x50%, then the production will be impacted by 50%. But, if the pressure from one train is not sufficient to feed train1 and train-2 compressors simultaneously, then the production will be impacted 100% even in 2x50% configuration.

For our process in consideration (Figure 1), where we have assumed duty-standby configuration for the two trains, the following two cases are possible:

a) Either the operator will have adequate response time available (including fault finding, decision making then field action) before normal liquid level reaches to the LAHH level, to reset the spurious low-level trip; or,

b) The operator will not have adequate response time available – in this case High-high level in V-1001 will lead to train-1 shutdown, which, may further extend up to the production well shutdown.

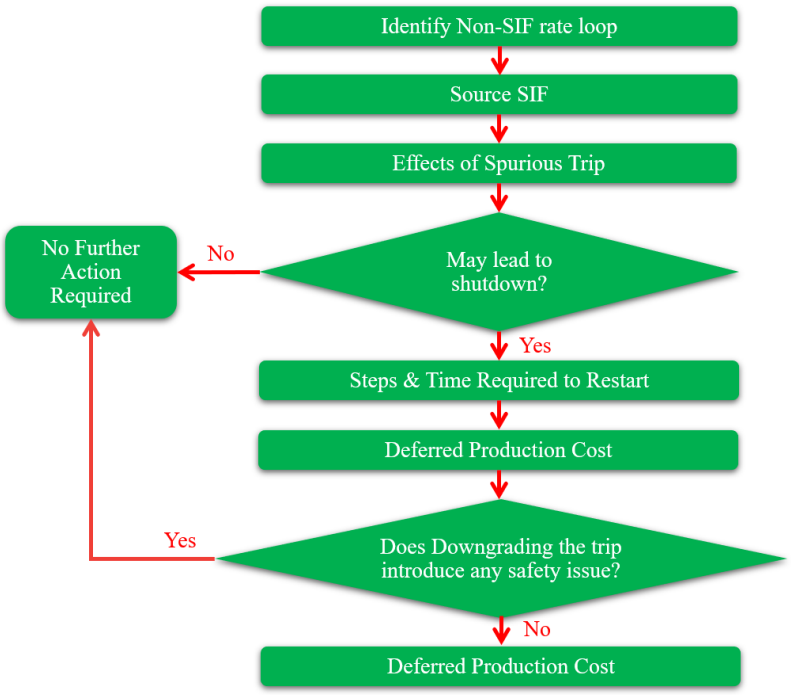
Evaluation of potential deferred production and its monetary value is presented in Table 7, based on the time to re-start presented in Table 4. The recommendation in this scenario will be to change functionality of LT-1004 loop from high-high level ESD trip to an alarm in DCS. As risk reduction measure does not recommend providing extra prevention or control measures, a CBA is not required in this case.

It is again worth mentioning here that the 2nd stage separator is designed to maximum operating pressure in the 1st stage separator. Therefore, there will be no safety compromises by this change. However, for more complex cases, the resulting change in risk profile shall be assessed. This step will be akin to reverse hazard identification – starting from the existing risk control measure and back-assessing the risk if the control measure was not available. Assessment of risk will be carried out assuming that a) risk control provided by the source element under consideration and the corresponding safety function is not available, and b) all other existing safety controls are available as per the as-built or in-field status. The resulting risk shall then be compared against the company's risk tolerance criteria. The methodology is schematically presented in Figure 3.

Table 7: Evaluation of Scenario 3

Equipment	Source SIF	Failure Mode	Frequency of occurrence per year, (F)	Sequence of Events	Expected duration of plant outage (hrs)	Total planned production (BBLs) per day	Total Deferred production Loss (USD) 60 USD/BBL per year	Recommendations
(25% IRR)								
1st Stage Separator (V-1001)	LT-1004	Malfunction of LT-1004 showing level high but actual level is normal	0.1	Leading to Level 2 shutdown (ESD-2)	3	5000	938	Change ESD trip (LALL-1004) to alarm (LAL-1004) in DCS.
(75% IRR)								
1st Stage Separator (V-1001)	LT-1004	Malfunction of LT-1004 showing level high but actual level is normal	0.1	Leading to Level 2 shutdown (ESD-2)	3	5000	2813	Change ESD trip (LALL-1004) to alarm (LAL-1004) in DCS.

Figure 3: Methodology for Evaluating Scenario 3



Scenario 4: Review of production critical items to be provided with emergency power

Items, which are non-safety-critical or are not a major equipment, may sometimes be left out of emergency load assessments. However, such items, if not available in a power outage event, may sometimes lead to a plant shutdown. The section aims to highlight the importance of a thorough review of emergency loads, taking due cognizance of the non-safety critical, yet production critical items. This is presented through an example of produced water pumps, again referring to the process presented in Figure 1.

A quick and simple methodology for this review may involve considering each process stream on the facility PFD. Each process stream shall be followed through, looking for possible bottlenecks, which may be caused upon loss of power. Once this assessment is completed, a list of items, which shall be on the emergency load shall be prepared. The list shall then be compared with the existing emergency load list for a gap assessment.

This methodology is further explained using the process shown in the figure 1, based on a past study carried out.

Following the process between the facility boundaries, the following process streams are identified:

- 1st stage gas stream: Starting with the gas stream and 1st stage separation, following the routing up to gas export, no equipment was found to be critical in terms of power failure.
- 2nd stage gas stream: This gas stream passes through compressor before joining the gas export pipeline. In case of power outage and compressor not being available, pressure will start building-up in the 2nd stage separator. This will cause the PCV (PV-1006A) to lift. However, as this PCV is not designed for full flow blocked outlet case (Table 1), the pressure build-up may escalate. The escalation in pressure build-up may potentially lead to closure of SDV-1002. This will lead to plant shutdown (ESD level 2) as explained in scenario 2. To prevent this scenario, either of the following two recommendations can be raised:
    - Either include compressor in the emergency load list; or
    - Design PV-1006A for full flow blocked outlet case.
- Crude oil stream: During the design review it was assessed that the main and booster oil export pumps were already on emergency load. No further issues were identified for this case.
- Produced water stream: for this stream, it was identified that the produced water pumps P-2001A/B were not on the emergency load list. Failure of power to these pumps will lead to level build-up in the produced water tank TK-2001. Now that the water outlet is blocked, the oil and water comingled stream will find its way to export route. It should be noted that although, the level control valves will fully open, they are not designed for the comingled stream. This scenario can further lead to high level trip in the separators, if operator action cannot be taken in required time. To prevent these potential scenarios, produced water pumps shall be included in the emergency load list.

For a facility where authors were involved in a similar exercise, it was identified that motor operated valves were used for shutdown functions. But, for the sake of brevity, discussion around the Motor operated valves in critical service is not discussed here.

Scenario 5: Common equipment shared for identical trains

Common equipment, as the name itself suggests will lead to production being compromised from all the trains in case of any leaks or upsets therein. In our example (figure 1) the common equipment are 1st and 2nd Stage Separator KODs (V-3001 / 3002). Potential process issues with these KODs have already been discussed under the previous scenarios.

In addition, common equipment obviously lead to shutdowns of all the relevant trains during upsets, inspection or other maintenance activities.

Scenario 6: Operator error

Operator errors during maintenance or testing of critical elements e.g. fire and gas detection can also lead to plant shutdowns, even with depressurization. These types of errors can be prevented with proper training, competence and safety culture. The other latent causes may be factors owed to limited information being available status of the plant,

Adequate training may enhance capability of an individual to perform the required task. Event analyses have shown that more human errors occur "in the field" than inside the control room. To address this concern, personnel in direct contact with equipment need additional training to familiarize themselves with the working environment, interactions and restrictions regarding other equipment and facilities, operation and maintenance of equipment designed to prevent unintentional trips during plant operation.

A high level guidance regarding some areas that shall be covered in designing the training for maintenance personnel is provided below:

1) Awareness about criticality of the subject system to be maintained;
2) Standard Operating Procedures and method statements;
3) Sharing lesson learned and sensitize operating personnel to the problem;

4) Testing and Maintenance conditions including stage wise mandatory checks;
3) Simultaneous Operation and Impact if recommended controls are not followed;
5) Transient and Operational conditions;
6) Proper use of tools;
7) Safe system override training;

In addition, in-field and hands-on competency assessments shall be incorporated in the contractor selection and training.

Conclusion

Even for low production rates the cost-benefit ratio is much lower than the selected criteria of <2, for adopting a a recommendation. The operations teams can use these results or methodology as a back-up case or justification for a change request. It shall be noted that the chosen criterion of cost-benefit ratio <2 is on the lower side to start with. Hence, it is easily demonstrated that the benefit of implementing risk control measures in this assessment, or a similar exercise will far outweigh the potential deferred production or operational nuisance. The cumulative impact of implementing such recommendations across the facility can easily make the effort and cost of carrying out such rationalisation studies.

However, such studies or reviews are highly dependent upon the level of preparation and competence of the team. Therefore, facility owners shall commit adequate time resources within their teams responsible for such an assessment. In case the reviews are outsourced to a third party, then a robust contractor selection process shall be in place.

The assessment presented in this paper is for rationalising plant downtime issues. However, the holistic approach and system thinking presented, can also be applied in revalidation of revalidation of process hazard analysis studies such as HAZOP and SIL assessments, after making suitable adjustments to the assumptions and criteria used in this paper.

References

1. Health and Safety Executive (HSE), UK, “Cost Benefit Analysis (CBA) checklist”, accessed at https://www.hse.gov.uk/managing/theory/alarpcheck.htm on 1st September 2021.
2. International Electrotechnical Commission (IEC), “Functional safety - Safety instrumented systems for the process industry sector - Part 3: Guidance for the determination of the required safety integrity levels – IEC-61511-3, 2016.