

HYDROCRACKER SIL SELECTION CASE STUDY

Edward M. Marszal, P.E., C.F.S.E.
Principal Engineer
Exida
5561 Maleka Court
Columbus, OH 43235
emarszal@exida.com

KEYWORDS

SIL Selection, Hydrocracker, Depressuring, Quantitative Risk Analysis, QRA, Safety Integrity Level

ABSTRACT

The emergency depressuring of Hydrocracking process units in refineries has received a large amount of attention after the accident that occurred at the Tosco Avon Refinery in Martinez, California. Many refiners decided that automatic depressuring of the unit when excess temperature was detected should be a safety instrumented function. Refiners found that applying this safety instrumented function is quite difficult due to the large number of measurements that are possible and the difficulty in detecting the hazardous condition.

This paper presents a case study of the selection of a safety integrity level for the depressuring function. The case study is of interest because of the advanced methods that were required to provide reasonable results. Although simple methods are available and promoted in SIS standards, those methods provided results that were unacceptable in this situation. This paper not only provides the results that were obtained in the study, but also provides an overview of some of the more advanced techniques that can be applied to the SIL selection process along with guidelines for when more advanced techniques should be used.

INTRODUCTION

Safety Integrity Level (SIL) selection is the process of determining the amount of risk reduction required to reduce the risk that is posed by a process to a tolerable level. The SIL selection process has received a great deal of attention in the literature. The IEC 61511 standard alone contains five different methods for selecting SIL. These methods all perform the same task in essentially the same way. The differences in methodologies are a function of the level of detail in which the components of risk are analyzed. The detail ranges from a simple categorization of consequence and likelihood when using the hazard matrix method all the way to numerical analysis of event frequency and probable loss of life resulting from the accident when using a fully quantitative method.

Quantitative Risk Analysis (QRA) for the purpose of selecting SIL is rarely done. QRA requires highly trained analysts and increased effort when compared to qualitative methods. In addition, using the numerical results that are generated by the method requires that decision guidelines that are also numerical. Many organizations do not desire to have numerical representations of either the estimated

level of risk posed by a plant or the level of risk that the organization is willing to tolerate, due to the perception of liability that is created.

Even though QRA is not widely practiced for SIL selection, there are some situations where all of the other SIL selection methods, which are essentially various degrees of shortcutting QRA, are inadequate and will lead to artificially inflated requirements. In these situations, the selected SIL was higher than expected and deemed to be unjustified. An excellent example of this situation is the emergency depressuring of a Hydrocracker reactor section upon detection of a thermal runaway. In order to improve SIL selection, a limited amount of QRA should be incorporated into the SIL selection process for decision support. The key to effective implementation is only use small amount of QRA calculations to support your existing processes instead of trying to use QRA for every scenario.

HYDROCRACKING PROCESS AND HAZARDS

Many refineries employ Hydrocracking technology to convert heavy hydrocarbon oils into lighter and more valuable products. Figure 1 presents a typical flow sheet for a single stage Hydrocracking process^[1].

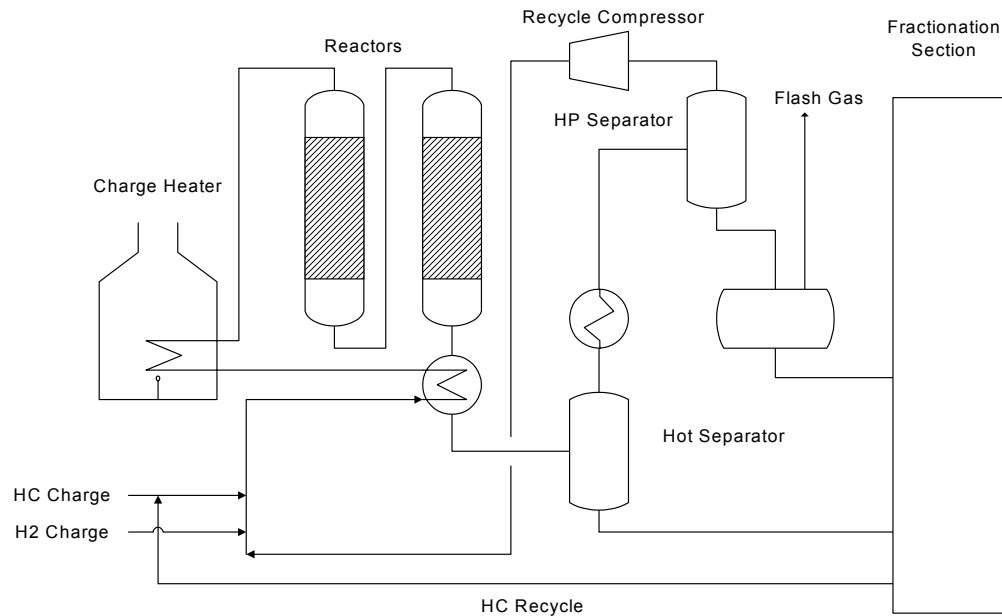


FIG. 1 – TYPICAL HYDROCRACKER FLOW SHEET

The Hydrocracker unit is fed with hydrocarbon liquid and hydrogen. Hydrocrackers are capable of processing a wide range of liquid hydrocarbon feed stocks, but typically process heavy oils such as vacuum gas oils and atmospheric residuals. The hydrogen / hydrocarbon feed blend is typically heated in a fired heater and sent to the reactors where the cracking reaction occurs. After heat exchange, the hydrocarbon products are separated from hydrogen and light gases in a series of separators and flash drums. Hydrocarbon products are further processed in a fractionation section. Both heavy hydrocarbon liquids and hydrogen may be recycled.

The reactions taking place in the Hydrocracker process include cracking, whereby long chain hydrocarbons are broken into smaller chains, and hydrogenation, where any free radicals or double bonds are saturated. The end result is a hydrocarbon product whose average molecular weight is much smaller than the molecular weight of the feed. The overall reaction set is significantly exothermic. Under some circumstances, there is a possibility that the heat generated in the reaction will increase the temperature of the catalyst bed, leading to increased reaction rates and more heat generation. This effect can spiral out of control and result in a potential loss of integrity of the reactor vessel or piping due to excessive temperature.

The reaction occurs as liquid hydrocarbon contacts a fixed bed of catalyst with excess hydrogen at a high pressure. During normal operation, adding a cold hydrogen quench to sweep away the heat of reaction to the downstream heat exchangers controls temperature. In an emergency situation depressuring the reactor can stop the reaction. When a depressuring occurs, the reactor pressure and thus the partial pressure of hydrogen decreases. The decrease in hydrogen partial pressure essentially decreases the concentration of reactant available, and in accordance with traditional chemical reaction kinetics, the reaction rate quickly falls off. The speed at which the reaction rate falls is a function of how fast the reactor pressure drops. Many Hydrocrackers are equipped with two different means of depressuring: a slow system, and a fast system. Obviously, the fast system is capable of bringing the process to a safe state more rapidly, but causes unwanted side effects such as intense flaring and equipment degradation due to hydrogen embrittlement. In an emergency scenario, an operator will first attempt to bring the process under control using the slow depressuring and only use the fast depressuring system if the other is not capable of stopping the runaway reaction from continuing.

For the case study scenario, a Safety Instrumented Function (SIF) that will initiate a fast depressuring upon detection of a high temperature condition in the reactors will be analyzed. This analysis is complicated by the fact that there is an additional SIF specified which causes a slow depressuring upon detection of low of recycle hydrogen flow. These two SIF prevent the same hazard from occurring, but do not completely overlap because the low recycle gas flow SIF does not protect against all of the possible initiators of runaway reaction.

BASIC SIL SELECTION PROCESS

The owner of a Hydrocracker process used a standard process for selecting SIL. The process is based on a hazard matrix that was modified to include qualitative analysis of layers of protection. The process includes the steps shown below.

1. Select the consequence category
2. Select the category representing likelihood of the initiating event
3. Determine the required degrees of risk reduction based on the hazard matrix shown in Figure 2
4. Determine the number of independent protection layers^[2]
5. Calculate the required SIL by subtracting the number of independent protection layers from the required degrees of risk reduction.

The hazard matrix shown in Figure 2 is a typical example of a matrix that might be used in industry. In addition to qualitative descriptions of categories, such as “Severe” and “Rare”, the categories are also associated with quantitative ranges. This paper will demonstrate that inclusion of quantitative ranges in

qualitative tools, such as risk graph, will allow decision support through quantitative calculations. The example shown below was calibrated^[2] using tolerable risk guidelines suggested by the UK Health and Safety Executive^[3].

| | | | | | | |
|-------------------|--------------|-------------------------------------|------------|-----------|--------------|---|
| | | Frequency Range (per year) | | | | |
| <i>Likelihood</i> | Frequent | 10 - 1 | 3 | 4 | 5 | 6 |
| | Moderate | 1 - 0.1 | 2 | 3 | 4 | 5 |
| | Infrequent | 0.1 - 0.01 | 1 | 2 | 3 | 4 |
| | Rare | 0.01 - 10 ⁻³ | --- | 1 | 2 | 3 |
| | Remote | 10 ⁻³ - 10 ⁻⁴ | --- | --- | 1 | 2 |
| | * Calculated | 10 ⁻⁴ - 10 ⁻⁵ | --- | --- | --- | 1 |
| | | Consequence Range (PLL) | | | | |
| | | 0.001 - 0.01 | 0.01 - 0.1 | 0.1 - 1.0 | 1.0 - 10.0 | |
| | | Minor | Serious | Severe | Catastrophic | |
| | | <i>Consequence</i> | | | | |

* This category should only be used when supported by quantitative frequency calculations

FIG. 2 – TYPICAL HAZARD MATRIX

SIL SELECTION PROCESS PROBLEMS

While the process owner was very successful in applying the procedure shown above, a small percentage of scenarios that were analyzed (<5%) did not yield satisfactory results (e.g., the selected SIL was higher than expected, based on judgment). The process shown above, and all short-cut risk analysis methods, yields poor results when the assumptions upon which the process is built are not valid. For the case study scenario, the following considerations make the simple hazard matrix protocol ineffective.

1. There are a large number of events that can result in a runaway reaction (initiating events).
2. None of the initiating events has a significantly larger frequency than the rest that it can be treated as representative of the overall risk.
3. The safeguards that are employed in the process are not effective against all initiating events.
4. There is a large number of SIF that are intended to prevent essentially the same hazardous event.
5. Multiple SIF share common equipment
6. BPCS protection functions share final elements with SIF.

7. Many of the SIF are not 100% effective in preventing all of the initiating events from propagating into an accident.
8. There are mitigating events that decrease the probability of the occurrence of an accident that do not fit the description of an independent protection layer as given in the SIL Selection Guidelines.

SUPPORTING SIL SELECTION WITH FAULT TREE ANALYSIS

Based on the reasons stated above, the SIL selection team requested a detailed Fault Tree Analysis (FTA) to determine the estimated frequency of occurrence of this event. The SIL selection team agreed on a consequence category of “severe” qualitatively, and did not request further analysis. The result of the FTA was then used to select a likelihood category, and subsequently the required SIL.

In general, a FTA is performed by identifying all of the basic events that can either be the root cause of the accident (i.e., initiating event), or can prevent the initiating event from propagating into the unwanted accident. It is important to note that the term “DCS Protective Function” is used throughout the discussion as a description of a layer of protection. When this term is used, the system that is being described is a basic process control system (BPCS) function that is separate from the SIS that is under study. The basic events are then logically related to each other using a graphical representation. The result of the fault tree analysis is the frequency, or probability, of the “top event” or unwanted accident, which is calculated using the probabilities and frequencies of the basic events and a graphical description of how they are logically related. Information about the complete fault tree analysis is presented in the Appendix. The SIL selection team determined that there are nine initiating events that can cause a runaway reaction if no mitigating actions were taken after those events occurred. The events are shown below.

1. Recycle compressor failure

When a recycle compressor failure occurs, the flow rate of hydrogen through reactor decreases. The decrease in hydrogen flow rate effects both the hydrogen-to-hydrocarbon ratio of the feed and also will stop the flow of quench gas. When this occurs, the heat removal with excess hydrogen stops, but the reaction continues to occur because there is still ample hydrogen available at a high pressure. Since the rate of heat removal loss is so great it is virtually impossible for an operator to prevent a runaway reaction from starting. Therefore, this scenario requires depressuring. Depressuring will either occur due to the low recycle gas flow SIF, which activates the slow depressuring upon loss of recycle flow, or manual activation of the slow depressuring.

2. Reactor internals failure

The failure of reactor internals, such as catalyst support screens and distribution boxes, can result in a temperature runaway. Failure of equipment located above a Hydrocracking catalyst bed will result in debris resting on top of the bed. The debris will cause flow maldistribution and channeling. As a result, the areas of the bed where flow has decreased will suffer a decrease in heat removal and increased temperature. The increased temperature may propagate into a runaway reaction. The thermal runaway in this scenario is much slower to develop than for the recycle compressor failure scenario. As a result, automatic control and operator intervention have a good chance of being able to prevent a runaway reaction by adjusting quench rates to the effected bed. While recovery from internals failure is possible,

in some cases the damage is so severe that recovery is impossible and a depressuring must occur to bring process to a safe state.

3. Quench failure

Failure of quench control resulting in low or no quench flow could occur as the result of either controller failure or quench control valve failure. In either case, reactor temperatures would rise at a moderate rate as a result of loss of heat removal. Recovery from the failure is possible either through manual operation of the control valve from the control room, or hand jacking the control valve in the field if control room operation is not possible.

4. Plugging and channeling due to coking and contamination

During the normal course of operation of the Hydrocracker, coking and plugging will occur in all of the catalyst beds. Coking and plugging can result in misdistribution of flow and channeling through the catalyst bed. As channeling occurs, heat removal from the catalyst bed will lose its uniformity, allowing hot spots to occur in areas where flow has decreased. The increased reaction in hot spots can result in a temperature runaway. The development of temperature runaway in this scenario is quite slow compared to other initiating events, allowing automatic control and operator intervention to prevent the runaway in most cases.

5. Improper catalyst loading results in channeling

Plugging and channeling can also occur as the result of poor catalyst loading. The mechanism for runaway reaction is identical to the mechanism described in the paragraph above. In this scenario, it is expected that the operator will not have enough information or time to detect the cause of the problem and the channeling could be quite severe. As a result, no credit for the operator being able to regain control of the process is given.

6. Bed temperature measurement failure leads to runaway

Failure of a bed temperature measurement can lead to a temperature runaway if the result of the failure is decreasing or stopping quench flow. An erroneous low bed temperature measurement will result in the automatic quench controller decreasing quench flow rate. The decreased, or stopped, quench flow will result in a moderately rapid temperature rise as the heat removal from the bed decreases. If failure of the temperature measurement can be detected, the reactor can be returned to normal operation by switching the temperature measurement used for control. In addition, manual operation of the quench valve from the control room will also prevent a runaway from occurring.

7. Failure of a recycle gas flow controller

Failure of the recycle gas flow controller in a position where flow is stopped or significantly reduced will result in a temperature runaway. This scenario will result in the same outcome as loss of the recycle compressor. In this scenario, there is an opportunity for recovery by operator intervention. Depending on the control loop's failure mode, the operator can take manual control of the loop either from the control room or the field.

8. Change in feed flow rate and/or hydrogen-to-hydrocarbon ratio

A significant change in feed flow rate can result in a temperature runaway due to rapid change of the hydrogen-to-hydrocarbon ratio. Significant changes in feed flow rate are the result of failures in feed flow controllers and feed pumps. The temperature rise that will occur in this scenario is moderately fast, but recovery is possible through automatic and manual adjustment of quench rates and readjustment of feed flow rates. In addition to manual and automatic attempts to recover control of the process, a DCS function can be employed to loss of hydrocarbon feed and subsequently perform a slow depressuring.

9. Failure of fired heater outlet temperature control causes high heater outlet temperature

Excessive temperature of the reactor feed can also result in temperature runaway, under certain circumstances. Excessive temperature of the reactor feed is possible as the result of a failure of temperature control of the charge heater such that maximum firing occurs. This failure may result in reactor inlet temperatures that are so high that maximum quench rates cannot bring the reactant temperature back down to the stable range. If this failure occurs, the operator has the capability of bringing the process back under control by manually operating the failed temperature control loop. If manual temperature control fails, the operator also has the option of manually stopping the heater, which will bring the process to a safe state.

All of the initiating events described above can result in a runaway reaction if the listed corrective actions are not taken. Once a runaway reaction reaches the point where normal control cannot be re-established, the process can be brought back to a safe state by either manual or automatic depressuring. As described above, there are two different depressuring systems, one for slow depressuring and another for fast depressuring. In order to minimize the negative impact of a depressuring on the process equipment, the slow depressuring is always attempted first.

A slow depressuring can be activated by a manual switch in the control room or by exceeding the high-high temperature, as determined by a DCS protective function. In either case, the slow depressuring valve is opened by de-energizing its associated solenoid valve. Even if the slow depressuring system is activated, there is a possibility that it will not decrease the reaction rate quickly enough to prevent the runaway from propagating. In this case, a fast depressuring will also be required to bring the process to a safe state. Although failure of the slow depressuring to stop a runaway reaction has been postulated, it has not occurred within the lifetime of the plant.

A fast depressuring can also be activated by a manual switch in the control room or by exceeding the high-high-high temperature, as determined by a DCS protective function. In either case, the fast depressuring valve is opened by de-energizing its associated solenoid valve. If a fast depressuring is attempted from the control room and fails, the depressuring can then be accomplished by opening a manual depressuring valve in the field.

A fault tree was developed that represents the information presented above. This fault tree was quantified based on a variety of information sources. Control system and instrumentation failure rates were derived from the online database of the Exida SILver™ SIL verification tool. Failure rates of large piece of process equipment were categorized using expert judgment and information presented in Figure 2. Other mitigating events probabilities were quantified using conservative expert judgment of the SIL selection team.

Based on the conservative estimates presented above, the frequency of a runaway reaction resulting in vessel or piping failure would be approximately 2.4×10^{-4} per year. For information about the full fault tree representing this scenario, see the Appendix.

It is important to note that the calculated event frequency makes assumptions about the integrity of SIF that are used to prevent the runaway reaction in various ways. The scenario under study contains two SIF that can mitigate a runaway reaction, depending on the initiating event that causes the runaway. Specifically, there is a SIF which will cause a fast depressuring upon detection of high temperature at the reactor outlet (this is the SIF for which this SIL selection analysis is being performed), and there is also a SIF that will perform a slow depressuring upon detection of loss of recycle gas flow.

When two or more SIF are used to perform to mitigate the same hazard; theoretically, there are an infinite number of combinations of allocation of risk reduction between the two SIF that will yield a valid result. Since the SIL selection process can only yield the required SIL for a single function, other means are required to allocate required risk reduction to one of the SIF. In this study, a SIL of 1 was assigned to the loss of recycle gas depressuring SIF, and then the SIL required of the high temperature depressuring SIF was calculated based on the residual risk. When more than one SIF is available to prevent a single hazard, all of the SIF except one should be arbitrarily assigned a SIL, and the balance should be “made up” with the remaining SIF. The “arbitrary” assignment should start out by assigning a SIL of 1 (i.e., lowest cost) to the SIF that is most expensive to install and maintain.

INCORPORATION OF FAULT TREE ANALYSIS RESULTS

The fault tree that was built and quantified represents the frequency at which the runaway reaction will occur without considering the SIF that is under consideration. The SIF under consideration is the high reactor temperature causes fast depressuring. The FTA resulted in a frequency of 2.4×10^{-4} per year. While some organizations have quantitative risk acceptance criteria that use this frequency result directly, those criteria are not required. In this case, the FTA results are simply used as support in selection of a likelihood category. The 2.4×10^{-4} per year figure falls into the “remote” category in Figure 2. It is important to note that the FTA result already incorporates the layers of protection that are available to prevent the initiating events from propagating into the unwanted accident. As a result, they should not be applied again. The required level of risk reduction obtained from the hazard matrix in Figure 2 is the required SIL for this scenario. Based on the calculated “remote” category for likelihood and the previously obtained “Severe” category for consequence, a SIL requirement of 1 for this SIF is obtained, based on the hazard matrix in Figure 2. The numbers in the hazard matrix represent the orders of magnitude of risk reduction that are required to make a given situation tolerable. Note that in some cases the required risk reduction can be 5 or 6. According to the SIS standards, SIS are only capable or performing up to 3 (ISA) or 4(IEC) orders of magnitude of risk reduction. If the analysis process yields a need for risk reduction of 5 or 6, this cannot be accomplished with a single SIF alone.

CONCLUSIONS

Short-cut methods such as hazard matrix and risk graph that are commonly used for SIL selection are effective in most situations (with some modifications). There are some scenarios where selecting SIL using these tools provides unsatisfactory results, usually because the selected SIL was significantly higher than original expectations. In these scenarios supporting these qualitative tools with quantitative calculations will provide more reasonable and accurate results. The results of the additional quantitative

analysis can easily be incorporated into the tool's format if inclusion of this type of analysis is planned during the construction of the tool.

The high temperature emergency depressuring of a Hydrocracker reactor is an example of a situation where the short-cut methods cannot provide a realistic result due to the complexity and interrelationship of the multiple safeguards and multiple initiating events. Use of additional quantitative analysis allowed SIL to be effectively assigned for the multiple SIF involved in mitigating this hazard.

APPENDIX

The full fault tree analysis is too detailed and lengthy to include in this paper. A complete copy of the fault tree analysis can be obtained by contacting the author by mail or e-mail at the address shown on the first page. The complete fault tree analysis is also available for download from the Exida web site at the following URL: <http://www.exida.com/articles.asp>.

REFERENCES

1. Meyers, Robert A., "UOP UNICRACKING PROCESS FOR HYDROCRACKING", Handbook of Petroleum Refining Processes, Second Edition, McGraw-Hill, New York, NY, 1997, 7.41-7.49.
2. Marszal, E.M., and Scharpf, E.W., Safety Integrity Level Section – Systematic Methods including Layer of Protection Analysis, First Edition, Instrumentation, Systems, and Automation Society, Research Triangle Park, NC, 2002.
3. United Kingdom Health and Safety Executive, The Setting of Safety Standards – A Report by an Interdepartmental Group of Advisors, Her Majesty's Stationery Office, London, 1996.