

CONSIDERATIONS FOR LAYER OF PROTECTION ANALYSIS FOR LICENSED PLANT

Jo Fearnley
Senior Consultant, Aker Kvaerner Consultancy Services, Aker Kvaerner, Ashmore House, Stockton on Tees, TS18 3RE, UK
E-mail: jo.fearnley@akerkvaerner.com

Chemical plants are routinely built around the world using a standard process design package supplied by the licensor of technology. Typically included in the package is the identification of the instrumentation to be included within the emergency shut down system, and the required safety integrity level identified for each safety instrumented function. These are presented as necessary requirements to meet the licensor's internal minimum safety standards. Other requirements to meet minimum safety standards are also often included, such as mandatory procedures. The input to, and detail of, the assessment on which these requirements are based is not provided within this licensed process design package.

This raises the question of what additional safety studies are required as part of the engineering design package. This will depend on a number and variety of factors; these will be discussed, with examples, and the implications for SIL assessment debated.

BACKGROUND

A licensed process design package (PDP) is rapidly becoming the most common basis for chemical plant expansion across the world. Tried and tested designs for producing a wide range of chemicals are licensed by technology owners, and the client pays a premium for the benefit of investing in a design which is known to deliver a quality product. The basic process will remain unchanged, although progressive improvements to equipment design or catalyst may be part of the evolution of the design over the years.

The actual scope of the licensed PDP will differ from one chemical to another as typically the PDP is targeted at those aspects of the design where a change to the base design could affect the end product. Hence, although the reaction and purification unit operations are fundamental to the process, other activities, such as raw material handling, raw material purification, catalyst charging, separation, recycle and product handling, may or may not be within the scope of the licensed process. It is therefore not possible to talk about the standard content of a PDP, and hence what will not be included.

When companies developed, designed, constructed, commissioned and operated their own process plants they were in control of the associated safety studies, even if a contractor was used for the detailed design and construction aspects. In such cases the progression of successively detailed hazard studies, such as the six stages of hazard study originally developed by ICI plc in the 1960s, was part of the standard design process for many larger companies. As a result these studies were well controlled, documented, monitored, and comprehensive.

However, with licensed plants the structured progression through a series of studies often gets lost in the development from front-end design to detailed design to construction to commissioning and eventually operation. The confusion is increased by the frequent switch between contract companies at the various stages, leading to a lack of continuity in both personnel and communication/information flow.

Underlying the requirements for safety studies at different stages in the design process is the information provided by the licensor and the standards required by the client. Between the two is the contractor, who needs to take great care to understand the discrepancy between the licensor supply and the client demand such that it is adequately covered in the bid and the programme. The risk is that in the commercial drive to reduce costs and win the contract this could be overlooked.

Dependent on the scope of the contract, consideration will need to be given to those aspects of the design within the PDP and those outside the licensor's remit, but within the contractor's remit; i.e. the off-plots. The situation is further complicated by elements of the design which are outside battery limits (OBL), i.e. to be completed by others, or already existing. There will frequently be differing safety, health and environmental (SHE) assessment requirements for the PDP, the off-plots and the OBL interactions. The usual situation is that the PDP will contain some integral hazard studies, whilst none of the off-plots will be covered, and information regarding the OBL interactions will depend on their build status compared to the licensed plant.

As part of my role as a risk consultant for Aker Kvaerner Consultancy Services I am routinely involved with the range of risk assessments required for licensed plants. One aspect of this consultation is the fundamental question:

'What safety, health and environmental assessments do we need to do?'

Unfortunately there is no single answer to this question as the combination of the licensor, the client, the contractor and the contract itself mean that every project is totally individual. This paper discusses the issues raised by this uncertainty when considering the requirement for safety instrumented functions (SIF) to comply with EN-61511.

In order to determine the safety instrumented functions for a plant, and the other design and operating aspects which provide prevention, control or mitigation of hazardous scenarios, a detailed hazard identification for the whole plant is necessary, which covers the areas within the PDP and those within the off-plots. It is not possible to cover the areas outside battery limits, but an awareness of impact on. and from. these is needed to be comprehensive.Once the hazardous scenarios have been identified, typically at an early stage in the project, the design should, where possible, provide inherent design features which eliminate the risk, or, where this is not possible, prevent, control and mitigate that risk. The assessment of the identified hazardous scenarios, considering the design of the plant, is frequently done using the layer of protection analysis (LOPA) methodology from EN-61511 for process plants, to identify the relevant protective features of the design and ultimately determine the instrumented systems which are required to have a safety integrity level (SIL) rating.

As a simplistic starting point it is normally the case that for a licensed plant design the section within the PDP will have the SIL ratings of the SIFs identified, whereas the off-plots will not.

PROCESS DESIGN PACKAGE – PDP

The licensor will have completed safety studies as part of the development of the PDP, and the design will also typically have been developed over the years to incorporate operational experience. However the PDP seldom, if ever, includes the SHE assessments in a form which is comprehensive and easily transferable between licensor and client. It is this lack of definitive documentation which leads to the question 'What safety, health and environmental assessments do we need to do?'

At any stage in the design process, the basic questions to ask are:

- What has already been done?
- What is available?
- What does the contract require to be done?
- What does good/best practice require to be done?
- What safety targets/risk tolerabilities are required/appropriate?

Unfortunately, just because a risk assessment has already been completed does not mean that it is available for direct use. For example the licensor will have a wide range of prevention, control and mitigation features built into the design of the PDP supplied. However what is often lacking is the full detail of the completed hazard assessments which lead to the design as it stands. A document commonly provided as part of the PDP is the list of alarms and trips for the plant, which need to be part of the independent safety system rather than part of the basic process control system (BPCS). For these instrumented safety systems the required safety integrity level (SIL) will also be provided within the PDP. The process trips within the design which are not subject to a SIL rating are those within the design of the BPCS. The detailed assessment which determined which are SIL rated and which are not is not normally available; only the output detailing those hazards determined by the licensor as requiring specific design or operational features will be available. This assessment is often referred to as the PDP layer of protection analysis (LOPA) document. The document is, however, not calibrated or quantified, but simply contains a list of scenarios and the requirements for associated procedures, alarms and (SIL rated) trips.

This is the fundamental cause of differences between projects, as for some clients it is enough to accept the standards set by the licensor, whilst others insist that their own company standards are applied to all new build projects. For the former the supplied design can be used as the basis for the project, whereas for the latter it may be necessary to complete all risk assessments to the client standards and hence alter the PDP if there is a discrepancy in integrity levels determined. For licensed technology it is part of the license that it is only acceptable to increase the safety functions, not decrease them.

The underlying factor which affects this is that the risk criteria on which the licensor has based the risk assessments are not typically available for comparison with the

standards of the client. Such risk criteria are often considered confidential and not something which a company wishes to be shared, as they are perceived as a reflection on the company concerned if they are not as restrictive as someone else's criteria. However to complete a safety integrity level assessment, either using a risk matrix or layer of protection analysis requires that the criteria for the boundaries between intolerable, tolerable and broadly acceptable levels of risk are quantified. The interaction between the frequency of an event occurring and the severity of that event will determine the risk arising from the event, and hence its acceptability. To reduce the risk the frequency and / or the severity needs to be reduced.

To compound the problem, it is normally obvious from the output data numbering which is supplied within the PDP LOPA report that there are a large number of scenarios which were in the original licensor assessment for which the output has not been supplied; i.e. only those scenarios deemed significantly hazardous to require instrumented systems, or mandatory procedures to address them are included. The problem with this approach is that it is therefore not obvious which other design or operational features have been assumed by the licensor as the protection against the various scenarios. The licensor's argument is that the requirements are built into the PDP, and hence provided it is designed to the stated requirements the other scenarios will be adequately covered. This is fine where the resolution of the risk is covered by an inherent protection feature, e.g. that the equipment design temperature is high enough such that it cannot fail, or the relief device is sized to relief the pressure safely, or a vent is routed to a flare to address environmental issues. However some of the basis of the risk assessment may be a function of the tolerable risk accepted by the licensor, or may be based on assumptions about the environs of the client's site which are not valid.

Included within the PDP LOPA are physical, mechanical and inherent layers of protection, as well as control and operational considerations, which may not be specifically highlighted as layers of protection. This means that if there are any changes to the standard design it is not immediately apparent whether the SIL requirements are affected, as the change could affect a scenario not identified as having a SIL implication in the licensor package. It is therefore very important that any change in the design from the basic licensor package is specifically assessed for related hazardous scenarios and hence for potential SIL requirements, which can only be done in conjunction with the licensor. Examples of these layers of protection include relief devices (pressure and vacuum), bunds, flare systems, vent headers, design conditions of equipment and pipework, restrictive devices and equipment types. Care needs to be taken with any change as in some cases what may appear a positive change, such as increasing the ground area of a bund, could have a negative effect as it could increase the size of a pool fire and hence the radiation effect.

LOCATION-RELATED FACTORS AFFECTING THE PDP SIL ASSESSMENTS

There are other general factors which may affect the licensor LOPA which has resulted in the identified SIL requirements. These include layout, geographical considerations, operating philosophy or population density. The risk criteria used as the basis for the SIL

assessments for the PDP will be based on a standard plant environment, and is very unlikely to have been adjusted for the specific environment in which the client plant will operate. Due to the lack of underlying information regarding those hazards which have been screened out, it is difficult to determine whether the client specific environment will change the risk assessment.

An easy location specific factor may the vulnerability of the client site to certain geographical effects, which will not be part of the basic design package. An example is if the client site will be in a region prone to earthquakes, in which case there will possibly need to be vibration/motion trips that initiate the shutdown of a hazardous installation that would not be in the standard licensor package. Alternatively if it is in a desert then sand may invalidate a particular protective measure such as a bund, as sand build-up may restrict the capacity available unless additional precautions are taken. A further example is if the site is in a region prone to flooding, which may block drainage routes leading to an unexpected pool fire.

Changes to the layout may affect the SIL classification identified for a particular risk, as the consequential effects may be different. For example, if the occupied building locations are changed compared to potential flammable release sources then this could change the number of people who could be at risk if an event were to occur. Consideration is needed not only of the plant to be licensed, but also any other production units which are close enough to have an inter-plant effect. Higher numbers of people could also be at risk if the plant is to be located near to a site boundary with a population living close to the external boundary.

Operating philosophy changes may change a SIL classification, as the exposure/vulnerability of the operating personnel may be changed. Modern plants are typically intended to be remote-operated, and as such have a low time at risk factor for certain events with a localised effect as a low proportion of time will be spent on site. However if a manual operating regime is planned then this layer of protection factor will not be valid.

It will be necessary to consider and discuss all these potential factors between the licensor, client and contractor to ensure that the final design appropriately considers the risks, and relevant SIL assessments may need to be reviewed to assess the validity of the data and hence the design basis of the PDP. Part of this consideration is the awareness that SIL classification is an order of magnitude technique, so a significant change is one which has an order of magnitude effect on the layer of protection analysis. This is complicated by the fact that the original LOPA may have identified, for example, a SIL 1 requirement for a SIF, but this analysis was right on the boundary between the SIL 1 and the SIL 2 result. Hence it is possible that a small change could move an assessment into the next level of required protection, and without the values used in the original PDP LOPA it is not possible to identify the scenarios where this is the case. This is further complicated where a scenario had not been SIL classified initially, and yet a change may take it to SIL 1.

Underlying all these considerations if the principle of whether the client/local directives require that the ‘as low as reasonable practicable’ (ALARP) or ‘so far as reasonably practicable’ (SFARP) principles are applied, and whether the licensor package utilises

these principles. This could add a significant level of complication to the discussions about acceptable risk criteria, and is highlighted here, but is not further discussed.

CONSIDERATION OF OFF-PLOTS AND SIF REQUIREMENTS – UTILITIES

The utility requirements of the site will be different dependant on whether the new plant is on a brown-field or green-field site; what facilities already exist; what is being built in the same timescale; and what the plans for the future are. As a result the utility requirements for a licensed plant are seldom, if ever, included in the basic PDP as the demands are endlessly variable. The effect of the local environment on the utility requirements also changes the specification significantly.

As such the only standard statement for all licensed plants is that the utilities will need to have a series of appropriate SHE assessments completed during the lifetime of the project, including a hazard identification process which will enable appropriate assessment of the risks identified to enable the SIL assessments to be completed. These will need to consider not just the licensed plant which is the subject of the project, but also the interactions between the other plants on the complex. Therefore even the scope of such studies will not be clear cut, as the utilities may be part of the off-plots or provided by the client or a third party as a series of OBL connections. In the latter case the safety studies will need to focus on what the project effect could be on the OBL plant, and what the potential effects of the OBL facilities could be on the project. Hence the critical aspect in this case is clear communication and two-way transfer of information to ensure that all mutual concerns have been addressed.

The utilities include not just steam, water, nitrogen, air etc, but also flare systems, waste treatment systems and pre-treatment systems as necessary. There can therefore be a significant scope in the utilities aspect of a licensed plant that needs to be considered.

For different projects the variability of licensor, client, contractor and stage in the process design will mean that it will not be certain that the SIL assessments will have been completed, so an initial check for the SIL assessment status at the transfer of a licensor project into a new stage is good practice.

CONSIDERATION OF OFF-PLOTS AND SIF REQUIREMENTS – RAW MATERIAL AND FINISHED PRODUCT HANDLING

The other areas which may fall into the off-plots scope are raw material and/or finished product handling facilities. Again this is because the scope can vary so widely between facilities, as it depends on what is already present. The supply of raw materials, for example could range from a supply pipeline from an upstream, integrated source, through to transport offloading facilities and significant storage, handling and purification systems. Catalyst and additive handling may be additional or inclusive in the PDP. The finished product handling is seldom included in the PDP as the requirements for storage or packaging will depend on the local infrastructure and transport situation.

As for the off-plots utilities these aspects of the off-plots will need appropriate SHE studies to be completed, including a hazard identification process leading to SIL assessments. The complexity and extent will depend on the hazards of the materials to be handled. These areas can be quite extensive for some process plants, and hence a significant amount of resource may need to be committed to the SIL assessments, and as for utilities the comprehensiveness of the SIL assessment data available needs to be reviewed when a project moves from one stage in the design process to another, and/or from one contractor to another.

PDP SIL REQUIREMENTS – SAFETY, ENVIRONMENTAL AND FINANCIAL

The SIL requirements indicated within the PDP LOPA report are based on the requirement to protect against human harm, and usually to protect against environmental harm as well. However, they will seldom, if ever, include protection against financial / asset loss. Therefore, in addition to considerations of the differences between client and licensor risk criteria for human and environmental harm, the contract needs to be very clear on whether there are risk criteria to be considered for financial and / or asset loss. The level of acceptable risk for financial loss is even more variable between companies than that for human harm or environmental damage. Consideration of financial loss can lead to significant changes in instrumented systems, typically around equipment which on catastrophic failure could lead to significant outage, loss of revenue and / or replacement costs whilst not necessarily having a high level of safety or environmental risk. This issue becomes even more complicated if there are reliability and availability clauses within the contract, as installing additional instrumented functions to protect against equipment damage could lead to spurious trips, leading to additional downtime. The cost of such instrumented functions can therefore escalate significantly if building in duplication and voting systems to get the correct balance between protection against failure to operate and protection against spurious operation.

ALARM RESPONSE AND CONTROL ACTIONS AFFECTING SIL REQUIREMENTS

There is one area which can have a significant impact on the PDP LOPA acceptability to a client. This is when the client does not accept response to an alarm as a valid layer of protection. This is not common, as the IEC 61508/61511 standards allow alarms and control actions to be considered as layers of protection where they are independent from each other, although with a limited probability of success, but there are companies where their internal standards are stricter than the IEC standards.

In this case all the relevant SIL assessments will need to be reviewed and alternative protection identified, or SIL requirements changed appropriately. However it is only for the scenarios identified in the PDP LOPA report where this can be readily achieved, and there may be other scenarios where the use of an alarm response has reduced the risk sufficiently for the scenario not to be listed. It is therefore necessary to have direct discussion between the interested parties to address the issue. Where direct response to an alarm is not

typically considered a layer of protection by a client this may be overcome by including a written procedure for the response to the alarm, to increase the integrity of response. However this is client dependent, and in reality the response time available between alarm and incident needs to be sufficiently long to enable a procedure to be accessed, read and acted upon for this to be a real layer of protection.

Another difference specific to certain clients is the number of layers of protection within the control system which it is acceptable to consider in a SIL assessment. Normal practice limits control systems to providing a maximum of two independent layers of protection, and care must be taken to assure true independence of these within the control system. Detailed consideration of the potential for common mode failure of the control system, which would affect the independence, is needed. Common mode failure mechanisms could occur due to a variety of causes, such as input/output cards, parallel cable routing, physical location, common equipment supplier or duplicated equipment types. It the client only accepts a single layer of protection relating to the control system, taking a pessimistic view the one failure could affect the whole control system, then a similar review to that detailed for the alarm response is required.

ACHIEVING SIL REQUIREMENTS FOR THE FINAL DESIGN

As the data is not available, it is often a subjective view as to whether the licensor package identified SIL requirements and other specified layers of protection are equivalent to those which would have resulted from a SIL assessment based on a client calibrated risk graph. One method to overcome this concern is to reassess a representative selection from the supplied PDP LOPA report, using the client risk criteria. If the assigned values seem to be comparable, then the assessment is usually accepted, but where it appears to be underestimated then a decision needs to be taken as to whether to complete a comprehensive, or partial, process hazard and SIL assessment for the design package, in order to satisfy the client internal standards.

To achieve the specification of the SIL requirements for the final design all the above aspects need to be consolidated into a single package. The use of LOPA to determine that a SIL rated safety instrumented function is required is just the start of the process. The actual achievement of the layers of protection identified is part of the detailed design package, considering the complete SIF design, equipment specification, installation, maintenance, proof testing, and auditing.

REFERENCE

Fearnley, J., 2007, Safety Integrity Levels – Considerations for New and Existing Assessments, 12th International Symposium Loss Prevention and Safety Promotion in the Process Industries, 2007, Edinburgh