HAZOP AND LOPA THE ODD COUPLE

C. Fare de Salis
Rowan House Ltd., 5 Hurst Green Precinct, Off Woodbury Road, Halesowen, West Midlands, B62 9RH, Tel. 0121 422 3311
South Wales Office: Tel. 01550 720711
North West Office, Tel. 0151 355 3588

Layer of Protection Analysis ("LOPA") is a complex calculation but according to the standard it is supposed to be a team activity. Can a complex calculation really be best undertaken in a team? This presentation arises from experiences with Chemical Engineers in the UK, Europe and in Canada.

Layer of protection analysis ("LOPA") is widely used for establishing safety instrumented system needs. LOPA is covered in IEC61511:3 Annex F wherein HAZOP is not mentioned once, nor twice, but ten times. LOPA is supposed to be based on HAZOP but if you went on a LOPA training course you wouldn't know that and you're given an implied message that SIL assessment and HAZOP are separate. What on earth is going on? Why does Annex F give the emphasis on LOPA being a team assessment using the HAZOP team whilst the training course presents it as a clever calculation by someone with a calculator and who is quite good at finding references for papers from the internet?

- In IEC61511:3 SIL Assessment is based upon HAZOP (see particularly annexes B and F)
- SIL assessment is a team activity (IEC61508:1 and IEC61511:1 – both normative)
- IEC61511:3 F (the annex on LOPA) defines the team makes and says:
- Only ONE member of the team needs expertise on LOPA (so by implication the rest of the team does not)
- The team MUST have experience and knowledge of the process plant being studied
- The team make up is the HAZOP team
- The issue with LOPA is how you properly draw out the information from the team to:
- Complete Safety Requirements Allocation phase
- Give all the basic information needed for the LOPA calculation
- Where does the emphasis lie in the standard?
- Is it on knowledge and experience of the process plant?
- Or is it on how many other academic papers can be found giving probability data?

The emphasis on SIL assessment leading to the calculation of the Probability of Failure on Demand average, or PFDavg, for the safety loop draws the reader of the standard away from remembering that it is a real process plant that is being studied. Layer of Protection Analysis, or LOPA, comes from IEC61511 part 3 Annex F and it is the most widely taught and used technique. In my experience the team gets so focussed on completing the calculation that they forget the importance of the allocation of safety layers (known as "Safety Requirements Allocation" in the master standard) at the beginning of the SIL assessment process. I also experience a confusion, both by those undertaking SIL assessments and those providing training, between the SIL assessment for Residual Risk of the process plant hazard, and the SIL assessment of the proposed safety loop design.

As chemical engineers we are the lead engineer in the Safety Requirements Allocation activity and the SIL assessment for Residual Risk. These are team assessments. Yet LOPA is a detailed calculation; why waste time going through it with people like the plant operator? It's complicated enough for the engineer doing the calculation, and people like the operators wouldn't understand it anyway! ... Now that I've made your blood boil a bit ... there is a very serious point behind such a rhetorical question.

Layer of Protection Analysis, also known as LOPA, is a calculation of the residual risk used to assess the requirements for safety critical instrument loops. It appears in the process industry guidance standard IEC61511 Part 3 Annex F and now also appears in generic form in the second edition of IEC61508 (the master standard), in part 5. The same LOPA technique can then be applied to calculate the SIL required for the proposed safety instrument loop.

The analysis requires a team assessment and yet the numbers involved, and the way the calculation is done, leads to a growing body of literature that emphasizes the calculation and ignores the team nature of the SIL

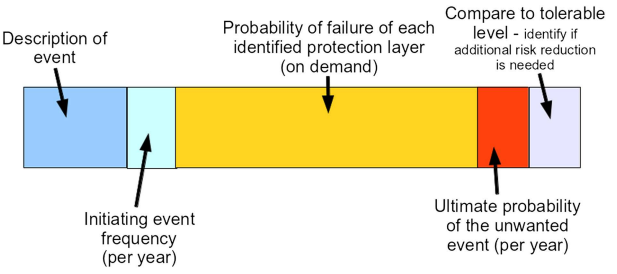
assessment . . . . which is odd, because IEC61511 Annex F is explicitly based upon HAZOP study, which is a team assessment of risk that includes people like the operator.[1]

The body of literature about LOPA is not un-influential. Take, for example, the research paper for the review of LOPA analyses of overfill of fuel storage tanks by Health & Safety Laboratories[2]: Throughout the paper, the numbers used in each of the calculations are heavily criticised, particularly in terms of the lack of supporting evidence, yet throughout the document there is no mention whatsoever of the Team assessment requirement from part 1 of the standard, and only one mention of HAZOP[3] as referenced in IEC61511 Part 3 Annex F. The consequence of documents such as these is that there is increasing emphasis placed upon using published data as sources rather than the knowledge of those who actually know the process plant and can offer their experience of the risk being analysed. The result is that LOPA becomes a mystical, complex calculation by a very clever person who can find all the academic references … without any serious reference to the HAZOP team that is required in the standard.

The structure of the calculation identifies how often the initiating event occurs and the probability that everything that acts against it might fail simultaneously leading to the unwanted event.

It can be a scary calculation to those not trained in LOPA when an example might look like this:

Structurally the LOPA can be understood as:



SIL assessment is based upon the idea that each risk event may have a number of properties of the process plant design and operation that reduce the unwanted event's likelihood.

The first layer of protection is the process itself.

As it says in the introduction to IEC61511 in Part 1 (page 13):

> *In most situations, safety is best achieved by an inherently safe process design. If necessary, this may be combined with a protective system or systems to address any residual identified risk. Protective systems can rely on different technologies (chemical, mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). To facilitate this approach, this standard*

1	2	3	4	5A	5B	5C	6	7	8	9	10
Impact Event	Sensitivity Level	Initiating cause	Initiation frequency (per year)	Probability of failure for the basic process control system	Probability of failure for the correct response to an alarm	Probability of failure of other technology risk reduction measures	Probability of failure of additional mitigation measures	Intermediate event frequency (per year)	Target event frequency (per year)	Is a safety instrumented system ("SIS") required (Yes/No)	PFDavg and SIL
Description of outcome	Grading of the outcome: Extensive, severe or minor	Failure of other event triggering the sequence of events	Frequency of event in column 3					Calculated by multiplying columns 4, 5A, 5B, 5C and 6 together	State the required target figure	If column 7 is larger than column 8 then a SIS is required	Divide column 8 by column 7 and determine the SIL
Overpressure of the vessel	*Extensive*	*PIC701 control loop failure*	*0.2/year*	*In column 4*	*0.3*	*0.1*	*Bund ignored*	*0.006*	*0.00005/yr*	*Yes*	*PFDavg= 0.00833 =SIL2*

- *requires that a hazard and risk assessment is carried out to identify the overall safety requirements;*
- *requires that an allocation of the safety requirements to the safety instrumented system(s) is carried out;*

Notice the emphasis on "inherently safe process design" coming first.

One of the key lessons from Flixborough was that the decisions we make about the chemicals used in the process, and the chemical inventories needed to achieve the desired production, directly impact on safety.

The second layer of safety is that of the operating conditions:

If my dryer has a risk of fire and explosion if the temperature goes above 140 deg C then an inherently

[1] IEC61511 Part 3 Annex F, Page 46:

F.1 Introduction

This annex describes a process hazard analysis tool called Layer of Protection Analysis (LOPA). The method starts with data developed in the *Hazard and Operability analysis (HAZOP study)* and accounts for each identified hazard by documenting the initiating cause and the protection layers that prevent or mitigate the hazard.

The author's emphasis has been added to the quotation. See also clause F.2 on the same page.

[2] "A review of Layers of Protection Analysis (LOPA) analyses of overfill of fuel storage tanks" by Colin Chambers, Jill Wilday & Shane Turner, Health and Safety Laboratory, Harpur Hill, Buxton, Derbyshire, SK17 9JN. HSE Research Report RR716, published 07/09.

[3] Page 10, Section 2.3.5, analysis of LOPA for company A in HSE Research Report RR716, published 07/09.

safer dryer will use steam at 105 deg C for heating instead of hot oil at 250 deg C. In the event of an emergency stop my drying material is in contact with a heated surface at 105 deg C rather than 250 deg C.

The third layer of safety is the structural and mechanical design of the vessels themselves. If a dust explosion pressure of sewage sludge is a maximum of 10 bar · g, then why can't we design and build some of the vessels to withstand 15 bar · g? If we could do so then we don't have a safety risk to the operators and maintenance staff because the hazard is contained.

It is the mechanical engineer's job to specify the required vessel design with the right corrosion allowance, the right materials of construction and the pressure rating of the vessel, the flange ratings etc.

The fourth layer of safety is the process control. If I have poor process control then I will often see high pressures or high temperatures, but if I have good process control then normally the control system will be able to cope very well and I will rarely get pressure and temperature alarms. The better the quality of the process control the less frequently I will have a dangerous condition.

The fifth layer of safety is that of the passive safety devices. These are devices that do not rely on any actuation device, electronics, motor etc.; so they include things like relief valves and bursting discs.

The sixth layer of safety includes both the powered, active safety devices like explosion suppression systems and the safety shutdown systems. These are the safety instrumented systems that we must assess and decide how many of them need to have a high degree of integrity.

Since this is the sixth layer of safety, then if the preceding layers offer a good degree of safety when compared to our target risk reduction, then the safety trip does not need to have a high integrity SIL rating.

SIL assessment for Residual Risk looks at the process design as a whole to decide if there is a residual risk to be covered by the safety instrumented system. So who is needed for the assessment?

Layer	Engineer
The process itself and the operating temperatures and pressures	Chemical Engineer and Process Chemist
Mechanical design	Chemical Engineer and Mechanical Engineer
Basic Process Control System	Chemical Engineer and Instrument Engineer
Passive (non-powered) safety devices	Chemical Engineer
Active, powered safety devices	Chemical Engineer and Instrument Engineer

Clearly, the approach is a team assessment by those who have good knowledge of the process plant. It is not, by contrast, a complicated calculation by some clever individual working in an office down the corridor with access to the internet from which he can find some interesting references.

The team involved in the SIL assessment is essentially the same team doing the HAZOP study.

What should be happening is that the HAZOP team discuss, review and assess each of the process plant risks and issue recommendations for consideration. That review is looking at all of the layers of safety that the process designers have included in the design.

Once the responses to the recommended actions are in, agreed and signed off what has actually be done is the "Safety Requirements Allocation" phase of the IEC61508 lifecycle. For example the team will have agreed that a relief valve is the correct safety device for covering the high pressure risk. Now the team view is analysed to see if there is still a left over residual risk to be covered by a safety instrumented function.

If that SIL assessment shows that there is a residual risk remaining then a safety instrumented loop is proposed and all risks covered by that loop are brought together to find the SIL required of the loop and its demand rate. That final SIL assessment also analyses the consequences of partial failure of the proposed loop which won't have previously been covered by the HAZOP study. For example, if the loop is required to isolate all lines into a process unit and shut it down and all valves act correctly except for the high pressure steam isolation then there is an additional risk now arising from a locked in plant into which HP steam is continuing to flow.

The team involved in the SIL assessment for the Allocation of safety protection layers ("Safety Requirements Allocation") and process residual risk is essentially the same team doing the HAZOP study.

Whilst part 3 of IEC61511 is guidance, part 1 of the standard is normative. The need for a team assessment for all of the assessment activities in the lifecycle is in part 1. IEC61511 Part 1 Clause 5 is about the Management of Functional Safety and I draw your attention to clause 5.2.6.1.2 which, at first sight, says something a little bit odd:

> ***5.2.6.1.2*** *The membership of the assessment team shall include at least one senior competent person not involved in the project design team.*
>
> *NOTE 1 When the assessment team is large, consideration should be given to having more than one senior competent individual on the team who is independent from the project team.*

This clause refers to the activities through the lifecycle of which the SIL assessment is part. The inclusion of a person with authority ("senior") who is competent and independent helps guard against going ahead with a poor design at all costs and that is understandable. However, the reference to a team that has amongst it one senior competent person (or a large team having more

than one), at first sight, seems odd. According to IEC61508 Part 1 clause 6 everyone involved should be competent. It becomes clearer when we look at what it means for LOPA in the SIL assessment stage.

IEC61511 Annex F clause F.2 says (page 46):

> ***F.2 Layer of protection analysis***
>
> *The safety lifecycle defined in IEC 61511-1 requires the determination of a safety integrity level for the design of a safety-instrumented function. The LOPA described here is a method that can be applied to an existing plant by a multi-disciplinary team to determine a safety instrumented function SIL. The team should consist of the:*

- *operator with experience operating the process under consideration;*
- *engineer with expertise in the process;*
- *manufacturing management;*
- *process control engineer;*
- *instrument/electrical maintenance person with experience in the process under consideration;*
- *risk analysis specialist.*

> *One person on the team should be trained in the LOPA methodology.*
>
> *The information required for the LOPA is contained in the data collected and developed in the Hazard and Operability analysis (HAZOP study).*

If the method requires a "multi-disciplinary team" and "One person on the team should be trained in LOPA" then, by clear implication, it is not necessary to have the whole team trained in LOPA according to IEC61511. Also the evidence for the decision is the HAZOP study, not some interesting academic reference that might, or equally might not, be directly relevant to your process plant application.

Papers and references are helpful where they are genuinely applicable to your process plant so I am not arguing that they have no place. I am noting that the emphasis in the standard is on the HAZOP process conducted by a team that has "*experience operating the process under consideration*". By contrast there is a growing trend for LOPA studies to emphasize the academic references and ignore the experience of the team, contrary to the standard.

We have enough trouble from SIL certificates and reliability data used for selling instruments being wafted around as evidence. The certificates look reassuring and the data looks good in a laboratory but it is all ignoring the real question about their applicability to your actual process. We don't need to go down the same road with the references used in LOPA calculations. There may be academic references to a valve failing open in a 12″ pipe that can be referenced in a LOPA calculation but that doesn't mean that the data is good for your 12″ pipe and your valve in your process plant.

Funnily enough the person with the most experience on the reliability of devices and the frequency of process upsets on the actual process plant being considered is the operator of the plant. When we look back at clause F.2 quoted above, who is top of the list? It's the "*operator with experience operating the process under consideration*". Indeed if you examine the list of those recommended for the team doing the study the emphasis is strongly on those who have experience of the process and not on those who have expertise in LOPA calculations.

So why is it that so much emphasis is today being placed upon how many academic references you can find to support your number used in the LOPA report, when the critical evidence is actually the HAZOP study?

Richard Gowland, Technical Director of the European Process Safety Centre, recently noted in an analysis of the final Buncefield report:

> "The accident report shows that there was a major deviation between the use of the control systems described in the [COMAH] report and the way they operated in real life, with the report stating: *"What was set out in the document and the safety-management systems did not reflect what actually went on at the site."*[4]

Perhaps those doing the safety risk analyses for controlling the major accident hazards should have asked the plant operators, i.e. those at the top of the list of clause F.2.

A move to put the emphasis on academic references for source data and moving away from tools such as HAZOP study as the basis of LOPA calculations would be a seriously retrograde step because we would be taking the most important person of all out of the loop: The "operator with experience operating the process under consideration".

Clive de Salis
15th March 2012

Clive de Salis is a registered safety professional with the I.Chem.E and was the first chair of the UK's 61508 Association. He is also a member of SIESO as well as being a chartered member of both the Institution of Chemical Engineers and the Institute of Measurement & Control. He is a member of GEL65/1, the BSi committee that writes IEC61508 and IEC61511. He is also the chair of The CASS Scheme Ltd and author of the I.Chem.E book "Using risk graphs for Safety Integrity Level assessment".

This paper and presentation is based upon a subject first discussed in outline with CSChE and also with InstMC.

[4] TCE, April 2011 issue, page 56, published by The Institution of Chemical Engineers.