A large Layer of Protection Analysis for a Gas terminal 2000+ scenarios/'cause – consequence pairs'

Richard Gowland
European process Safety Centre

- The scope of the study was a large gas terminal handling North Sea gas, condensates etc.,
- Supplying into Northern Europe Gas distribution
- Separation of LPGs and gasolines for shipment and sale.

This was a large upgrade project engineered by a major U.S. contractor on a site where the existing Protective Systems include:

- ❖ High Integrity Pressure Protection Systems (HIPPS)
- ❖ Process Shut Downs (PSDs) – plant control trips from control instrumentation
- ❖ Manual Emergency Shut down Systems (ESDs)
- ❖ Pressure relief to flare and atmosphere.

The object of the study was to answer the 2 questions: For hazard scenarios

– is there adequate prevention and protection to meet company and national requirements.
– If more protection is required, what form should it take and if Safety Instrumented Systems are required, what Safety Integrity Level (SIL) is needed?

Layer of Protection Analysis (LOPA) is a method which examines a scenario from its initiating events and their frequency, through all modifying probabilities, probability of failure of protective systems by simple calculation to see if a tolerable frequency of the final top event meets or exceeds requirements.

Setting the consequence severity tolerability levels

A key requirement of the LOPA methodology is to have severity criteria and target tolerability criteria agreed (injury/environmental/financial). This had been done by the owners and were generally in agreement with industry and regulator commonly adopted data for injury and fatality criteria. Company criteria were used throughout the study. An example of this was the adoption of a a frequency of 1E-05 for an on site fatality. It was agreed that the LOPA study team would define the severity for each scenario and case. This would then be assigned the standard target tolerated frequency to start the study.

A software tool based on Microsoft Excel ® was produced to calculate any protection gaps and record the studies as they proceeded. This had embedded in it all target frequencies, failure rates, conditional modifiers (probability of ignition, probability of exposure etc.) to ensure consistency and transparency. This would evolve into a single standard and tool for whole company.

- Wherever possible, we created standard consequence:
  - Injury/fatality
  - Cost
  - Environmental effect
- Agreed to always use worst case and carry out single 'line' study for each deviation (cause/consequence pair)

Initiating events - Failure frequencies

- Most were agreed at the outset and included in the software. These were 'process deviation causing events' such as process control loop element failure, loss of containment and human error. Some data used was 'generic industry taken from literature and some supported by company data

There was a concentration on process control deviations and equipment failures

- Level/flow/pressure/temperature control
- Heat exchanger tube failures
- Unplanned trips (turbines and compressors)

And some human error cases, e.g.

- Manually controlled systems
  - Tank level management
  - Loading/unloading
  - 'Pigging'

Modifying probabilities/Conditional Modifiers

Probability of ignition.

Hydrocarbon releases were assumed to ignite if their full potential was to be studied. Large releases were assumed to ignite 100% of the time. This was the default position when doubt was sufficient. Other smaller releases were assigned a probability of ignition based on physical properties, quantities, phase etc.

Probability of Exposure.

Was based on operational and geographical factors. For example a risk in a tank farm which is visited rarely and only for inspection would be considered for 1% or 10% probability of exposure. For very large events, again the default was always 100%.

In practice, during the study, conditional modifiers were rarely applied.

Protective Systems

Probability of Failure on Demand for Independent Protection Layers/Barriers:

- The following were normally considered:
  - Control systems
  - Process Shtutdowns (PSDs)
  - High Integrity Pressure Protection Systems (HIPPS)
  - Others (relief etc.)
- Wherever necessary Reference was made to IEC 61511, NL 'Purple Book' and National Gas Industry implementation standard.

As the study went on we created standard set of scenarios for each unit operation. The basic list of these operations is:

- **Loading/Unloading**
- **Storage**
- **Pressure let down stations**
- **Pigging stations (launching and retrieving)**
- **Mole sieves/Driers**
- **Heaters/re-boilers/coolers**
- **Distillation towers**
- **Reflux drums**
- **Pumps**
- **Compressors**
- **Turbines**
- **Knock out drums/flares**
- **Boilers**

The STUDY

Loading/Unloading scenarios/cases:

Primarily loading out (LPGs and Hydrocarbon liquids)

Failures on:

- level control
- Pumps
- Loading arms
  - Loading arm failure frequencies not readily available
  - Needed to estimate from company experience and extrapolating NL Purple Book data
  - Ship movement control
  - Human error

Discipline was needed on assumption about time at risk based on number of loading activities per year.

Storage: These are large storage tanks, cryogenic and ambient.

Storage System scenarios/cases: It was considered that since level is managed by operations the study primarily went into into overfill and overpressure cases.

- Refrigerated storage for LPGs.

  - ❖ Typical Initiators:
    - Loss of level indication
    - Wrong valve line up
    - Operator error

  - ❖ Independent Protection Layers (IPLs) and their Probability of Failure on Demand (PFD)
    - Level alarms 1e-01
    - Inflow trips via block valves 1e-01
    - Vent control to flare** 1e-01**
    - PSV Relief to flare 1e-02
    - PSV Relief to atmosphere 1e-02**
    - Position switches on valves 1E-01

    ** Care needed – not always accepted. Capacity may be limited or discharge not safe.

- Atmospheric storage (usually Floating roof) for flammable condensates etc.
  - IPLs
    - Level alarms 1e-01
    - Inflow trips via block valves 1e-01
    - PSV Relief to flare 1e-02
    - ***PSV Relief to atmosphere 1e-02 ****

  ***** Advised against this as IPL***

Fortunately – LPG stores were adequately protected without considering atmospheric relief as Independent Layer of Protection. The same was not true for atmospheric storage where it was found that relief would occur to tank roofs and lead to similar hazards to those seen at Buncefield with flammable liquids cascading down the sides of the tank.

'Pressure Let down' stations

Gas from offshore pipelines in at 160 bar and needed to be distributed into the gas terminal and processing units at lower pressures. This was achieved by conventional pressure control valves acting on signals from analogue pressure transmitters. In most cases the design pressure of the downstream equipment was much lower than the maximum available pressure and therefore pressure protection is required. Conventional relief systems are not appropriate. The pressure protection loops of interest usually comprised pressure switches connected to a logic solver and outputs to large fast acting block valves.

- Initiators – primarily failure of control valve loop.
- Independent Layers of Protection:

- Extensive use of High Integrity Pressure Protection Systems (HIPPS) which give tight shut off and containment and in a few cases relief to flare
- HIPPS function met requirements of Norwegian Gas industry and IEC 61511 requirements – PFD of 1E-02 normally used
- Hybrid systems sometimes used (so called secondary HIPPS) – incorporating control valve as final element. Changes were needed to allow testing – also name change. Reluctant to assign a value of better than 1E-01 to PFD.
- Valve Closure time on very large lines was an issue which eliminated some protection

The HIPPS system was already evaluated by reputable consultant and the principal findings supported LOPA team decisions.

Pigging Operations: The network of pipelines entering and exiting the terminal is routinely inspected and cleaned by the use of 'pigs'. The launching and retrieval activity for these necessitates opening the pipeline at 'pigging stations'. This activity is regarded as hazardous since it has the potential for large gas releases.

- Extensive protective systems
  - Limit switches
  - Mechanical locks
  - Block valves

  are used.

Since the equipment is very specialised and most actions are manual, most data was taken from experience and engineering judgement. The outcome was a strengthening of procedures to reduce failure frequencies.

Mole Sieves and Driers: These operations were primarily for quality control, however, accelerated corrosion could occur if the system failed.

- Operational Mode Failure consequences slow to build up and readily detected by quality testing
- Key hazard potential is in the regeneration process
  - Reactivity – exotherms
  - Overheating
  - Overpressure
- Initiating Events usually easy to define (control system failure)

Heaters/Reboilers/Coolers:

- Used industry or NL 'Purple Book' failure frequencies
- Exchanger design and pressure protection prevented system rupture
- Most hazard caused by high pressure gas into utilities - Almost always a protection gap resulted
- Outcome emphasised

- Mechanical integrity needs to reduce failure frequencies by eliminating known failure phenomena. Need to limit extension of inspection intervals justified by Risk Based Inspection (RBI)
- Action on final release points and leak detection to reduce potential consequences – not true Independent Protection Layers

Distillation:

- Very Large capacity trains
- Level and pressure control on feed forward from bottoms of each distillation column to inlet of next column in the train
- Potential to overpressure downstream equipment if level control is lost
- Level Control normally from displacement level controllers
- Pressure and Level scenarios more dominant than Temperature and Flow
- Independent Protection Layers
  - Alarms and trips from Pressure transmitters (independent of level control)
  - HIPPS
  - Multiple PSVs (PSV data checked on line during study – exploited high degree of design data availability – leading to re-evaluation of relief system)
  - Some concerns on independence – plant operators in the team were very quick to discover problems

Reflux Drums and Condensate Receivers:

- Level control deviations provided most scenarios which could over-pressurise the system
  - High pressure controlled by vent control to flare or in extreme circumstances, PSV to flare
  - Overflow
- Controls and trips generally shown to be adequate
- Level control deviations provided most scenarios
  - High pressure controlled by vent control to flare or in extreme circumstances, PSV to flare
  - Overflow
- Controls and trips generally shown to be adequate

Pumps:

- Key issues were:
  - Operation with closed valves
  - Seal leaks
    - Single
    - Double
    - Alarms
  - What are the severities of consequences?
    - Determined by size, potential ignition and location
    -

Compressors:

Hazards examined included leakage, catastrophic failures as a result of liquids in gas feeds.

- Mechanical and electronic machine protection devices to trip on vibration etc.
- Hazard cases protected by:
  - Liquid separation drums on inlet
  - Machine protection (vibration etc.) (not used as hazard protection in most cases)
- Surge conditions controlled by anti surge controls
- Settle out pressure upstream caused concern on compressor trips
- Concerns about machine protection being disabled by 'sharing' normal control system elements (Common Cause Failure re-design needed)
- Mechanical and electronic machine protection devices to trip on vibration etc.

Turbines:

Hazards examined included leakage, catastrophic failures as a result of liquids in gas feeds.

- Hazard cases protected by:
  - Machine protection (vibration etc.) (not used as hazard protection in most cases)
- Surge conditions controlled by anti surge controls
- Pressure ratings normally eliminated overpressure scenarios
- Concerns about machine protection being disabled by 'sharing' normal control system elements (Common Cause Failure re-design needed)

Knock out drums and Flares:

In these cases, the hazards studied were availability of flare in relief cases. Multiple relief requirements, liquid removal.

- All flares have knock out drums
- Knock out drums normally maintained empty
- Reliefs (PSVs) and pressure let downs (PCVs) discharge to knock out drums via headers
- All knock out drums have multiple alarms from independent field sensors
- High liquid level starts pump or opens drain – not usually taken as IPL
- Need high reliability operator response to level deviations since operator can be seen as a common cause of failure
- Serious consequences in fuel gas systems if liquid carryover
- Other ideas for trips/SISs?

Boilers:

Boilers are fired primarily on fuel gas from the terminal itself.

- Most boiler controls (Burner Management Systems) needed to be SIL2
- Serious concerns about fuel gas with liquid entrainment or gross quantities of liquid carry over into combustion chambers

- Some issues on hydrocarbons in condensate (detection and response)

Results and conclusions from the study

In all, there were more than 2000 cases studied by a team which was staffed by a leader, process engineers, instrument designer and operators. The LOPA methodology proved to be robust and was readily understood by all members. The plant operators quickly became familiar with the technique and were able to verify and in some cases dispute operational practices and the functional modes of plant operation. Their contribution proved to be vital. The use of simple excel based software was helpful since it ensured understanding and consistency of approach. There were occasional problems deriving failure frequencies and probability of failure of some unusual hardware systems, but this difficulty would apply to any method and not simply to LOPA. There were also some procedural issues around requests from instrumentation designers to assign a Safety Integrity Level (SIL) rating to every control or 'trip' loop in the facility. A) Managing Contractor Instrument department expected to start from a list of instruments – then to assign each loop with a SIL rating
Specifically, Plant Operations and LOPA chair expected to start with the deviations/consequences/scenarios – wherever possible using HAZOP as inputs

- Starting with deviations/consequences/scenarios
    - Addresses only those concerns which are significant
    - Connects to previous HAZOP studies
    - Cross check with Cause and Effect diagrams from instrumentation design to make sure no process related hazards missed
- Starting from a list of instrument loops
    - Large number of loops involved in process and quality control.
    - Process control items automatically included

This second approach was demonstrated to be unnecessary if the studies addressed all the hazardous scenarios and then include those instrument systems which were relevant.
Major lessons from the study were:

- In most cases, adequate protection appeared to be provided, but in a significant number of cases failed the independence or adequacy/effectiveness requirements
- Closing times for very large valves presented significant challenges.
- Management and procedures needed to be reinforced, documented and training given on tank level management and response to alarms
- The operating company's equipment records (design capacities etc.) were excellent and helped determine the adequacy of protection against studied hazards.
- Mechanical Integrity programmes for heat exchangers were very important in reducing failure frequencies, since there were few true independent protection layers available and protection was mainly in the role of consequence alert and reduction (e.g. gas detection)