



Practising Layer of Protection Analysis – LOPA rules and data limits

Richard Gowland, European
Process Safety Centre

My experience

- The Dow Chemical Company
 - Engineering (1971)
 - Projects (1975)
 - Production Management (1977)
 - New Technology (1984)
 - Process Safety (1989 -2003)
 - Standards and Requirements setting
 - Methodologies (Development of LOPA method and rules)
 - Risk reviews (multi level including LOPA)
 - Auditing
 - Training
 - Business Process Safety Leadership (Agrosciences)
- European Process Safety Centre leadership (2004 ...)
- Leader of Layer of Protection Analysis training course for I Chem E
- Layer of Protection Analysis for industry clients

LOPA basic rules

- 1 LOPA method and set of rules for the whole corporation
- Single software tool for whole corporation (this limits 'creativity')
- 1 single set of risk tolerance criteria (frequencies assigned to event scenarios)
- Technology leveraged scenarios and initiating events – hopefully no gaps
- Rules on 'independence'
- Conservative approach to 'Conditional Modifiers'
- Control of allowed initiating event frequencies and values assigned to layers of protection
- Strict quality criteria for acceptance of novel layers of protection
- Conservative approach to human factors

Sources of scenarios

- Seveso 2 Safety Report
- HAZOP study
- What if?
- Company scenario database
- Basic modelling of events (fire/explosion/toxic release) to support severity estimate

Risk 'Tolerance' criteria

- Review of published expectations from community and regulators and where available from industry
- Range from minor injury to single fatality and multiple fatalities
- Typical outcome $1E-05$ for single fatality on site
- Elevation of criteria for offsite effects (e.g. offsite fatality $1E-07$)
- Societal risks must be accounted for - based on (where available) company or published f/N curves

Initiating event frequencies

- Process Control system failures listed first then:
 - Utilities failure (power etc.)
 - Human error
 - Mechanical integrityOthers
- Process Control initiating events as IEC 61511
 - Care needed (rules) on how the Basic Process Control System logic solver is accounted for
 - Rules to make sure we don't violate general rule of independence when looking at layers of protection
- Human error conservative approach using HSE and other data

'Conditional Modifiers'

- Probability of Ignition (Fire/Explosion scenarios)
 - Criteria based on flammability (flash point, M.I.E. and quantity) e.g. any release >5000Kg probability = 100%
- Probability of Exposure of person/s
 - e.g. Tank farm operations 1% (rare) or 10% (normal)
 - Very large events (toxic release or explosion is taken as 100%)
 - Outside fence line exposure probability usually assumed 100%
 - Intermittent operation duration may be allowed e.g. unloading into a storage tank, but needs care when operational demand changes (Management of Change - M.O.C.)

Independent Layers of Protection

- Care needed to cross reference initiating event (e.g. loss of sensor means it fails control and any connected dependant alarm)
- Basic Process Control System trip to safe state
- O.K. if:
 - Initiating event is human error
 - Sometimes when initiating event is Basic Process Control System loop failed – rules needed – see later
 - Rarely when mechanical integrity fails – the cat is out of the bag – mitigation is last resort

General Rule on Independence

- Definition of an IPL: A layer of protection that will prevent an unsafe scenario from progressing regardless of the initiating event or the performance of another layer of protection.

Independent Layers of Protection

- Need to be:
 - Independent
 - Effective in returning plant to safe state
 - Tested (operators and mitigation devices are difficult to test)

BPCS trip as Independent Protection Layer

- When Initiating Event is Process Control failure

Consider if:

- Trip does not use any failed element in the scenario (sensor or final element) and signal and output are handled in channel separate from failed control (difficult to prove) or

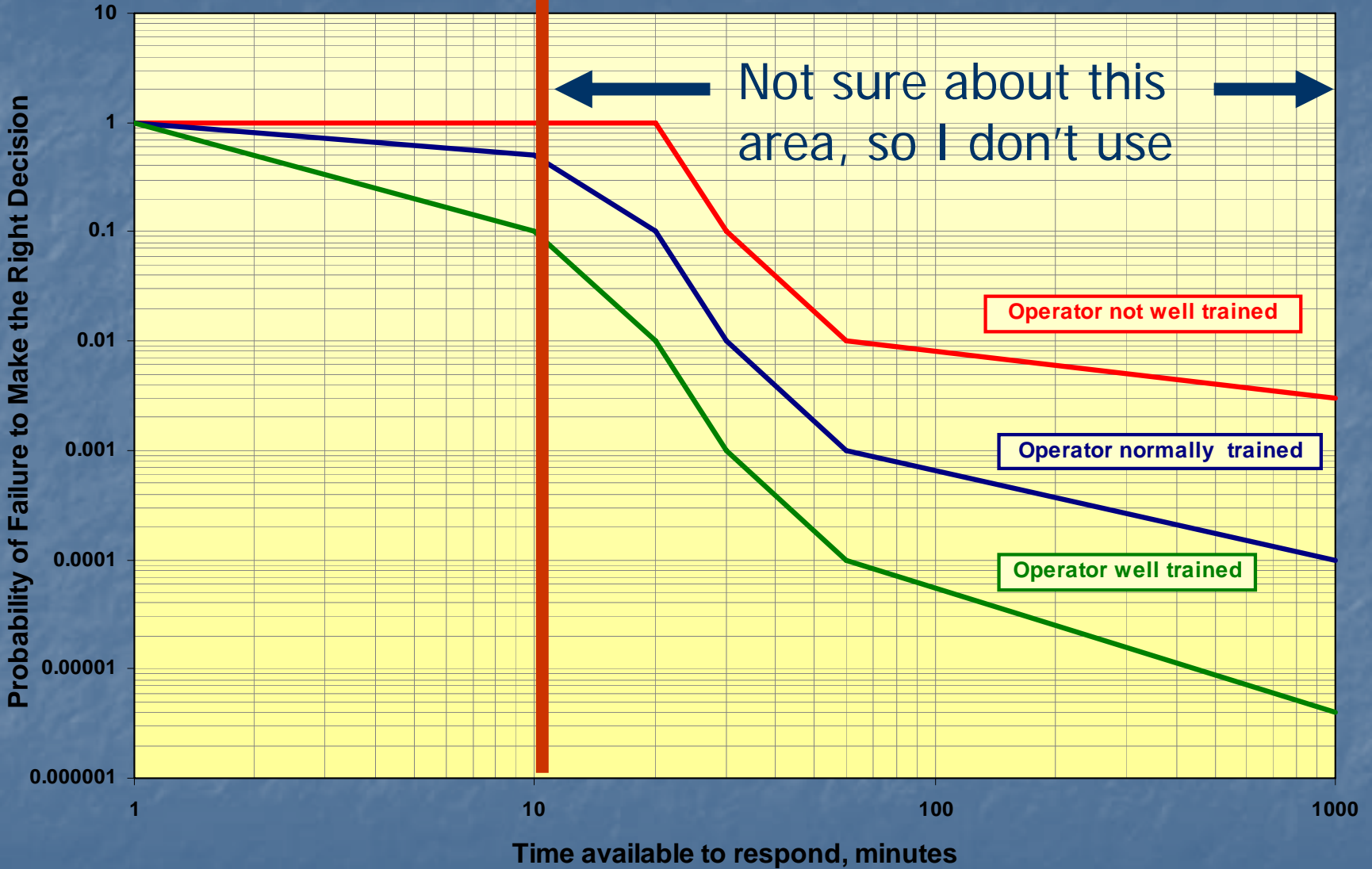
(SIL 2 BPCS logic solver makes this easier. (IEC 61511 pt 1 para 9.4.3). However these are rare beasts)

- Properly tested (whole loop)
- Limit PFD value to 1E-01

BPCS alarm as a Layer of Protection

- Don't use BPCS twice (trip and alarm) – alarm is not really independent if you do
- Operator must have time to hear, understand and act as response (<10 minutes not normally accepted unless part of emergency plan)
- Operator must be able to take plant to safe state without relying on any element of any other layer of protection
- If operator error is initiating event – don't take the operator as a layer of protection unless you have a behavioural science PhD
- Must test and record as a 'SIL 1 equivalent'
- Limit PFD value to 1E-01

Typical Operator Intervention as IPL



Relief and vent systems

- Only allow if:
 - Overpressure is scenario
 - Tested
 - Evaluated (bench test vs operating conditions)
 - Design data validated for scenario
 - no downstream consequence
- Limit value (normally 1E-02)

Safety Instrumented Systems

- Comply with IEC 61508/61511
- SIL1, 2, 3 normally in Process Industry
 - $1E-01 > \text{SIL 1} \geq 1E-02$
 - $1E-02 > \text{SIL 2} \geq 1E-03$
 - $1E-03 > \text{SIL 3} \geq 1E-04$
- SIL 1 has a very large range

Other Safety Related Protection Systems

- Proprietary trip systems with certified or proven in use PFD
- Limit 'creativity'

Management Systems

- Adherence to enhanced standards
- Enhanced Mechanical Integrity programmes
- Double check and sign off on Operating Procedures

May Reduce initiating event frequency –
care needed

Mitigation

- LOPA most easily copes with the left hand side of the 'Bow Tie' i.e. prevention
- Mitigation systems like fire protection or water spray for gas absorption/dispersion are difficult to test in real conditions if you are really convinced – consider adjusting incident severity
- Dikes and bunds normally considered in environmental scenarios

Taking all risks into account - advice

■ In LOPA

- use conservative 'tolerability' Target
- Restrict PFDs of non SIS IPLs to high end of PFD range
- When SIS is designed or assessed ,assume (conservative)
 - SIL 1 PFD = 1
 - SIL 2 PFD = 2
 - SIL 3 PFD = 3
- Formally address Uncertainty and Sensitivity

Uncertainty and Sensitivity

- Uncertainty – where is my data shaky and what is effect if wrong?
- Sensitivity – Which IPLs seem to be the most important and have the biggest negative effect if they fail (all eggs in one basket?)

ALARP

- Test for ALARP can easily be connected to study tool (done)
- Data shows.....

Reminder

- LOPA is 'order of magnitude' approach
- Does not routinely address cumulative risk from whole facility (sometimes enhanced to take account of several initiators for same scenario but that is all)
- Needs rules
- Has the right team in the room
- Needs trained facilitator and second party validation