Advances in Layer of Protection Analysis

Wayne Chastain, P.E.
Eastman Chemical Company

An AIChE Technology Alliance
CCPS
Center for Chemical Process Safety

Agenda

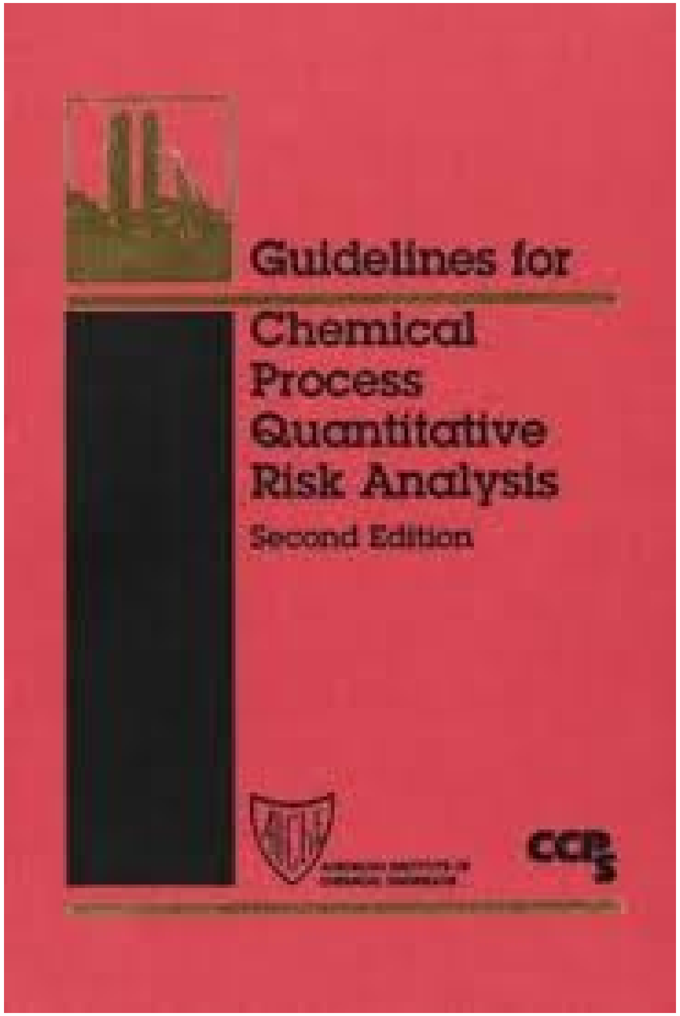
- Overview of Layer of Protection Analysis
- Guidelines for Initiating Events and Independent Protection Layers for Layer of Protection Analysis
- Guidelines for Enabling Conditions and Conditional Modifiers for Layer of Protection Analysis
- Path Forward – Evergreen LOPA Database

Layer of Protection Analysis

- Simplified form of quantitative risk assessment
- Uses order of magnitude categories for:
  - Consequence severity
  - Initiating event frequency
  - Likelihood of failure of Independent Protection Layers (IPLs)
- Provides a numerical indication of adequacy of protective systems

Quantitative Risk Analysis

- QRA is a suite of techniques for both consequence and frequency analysis
- QRA typically involves evaluation of individual risk and/or societal risk from a broad range of events at a plant site



Guidelines for Chemical Process Quantitative Risk Analysis

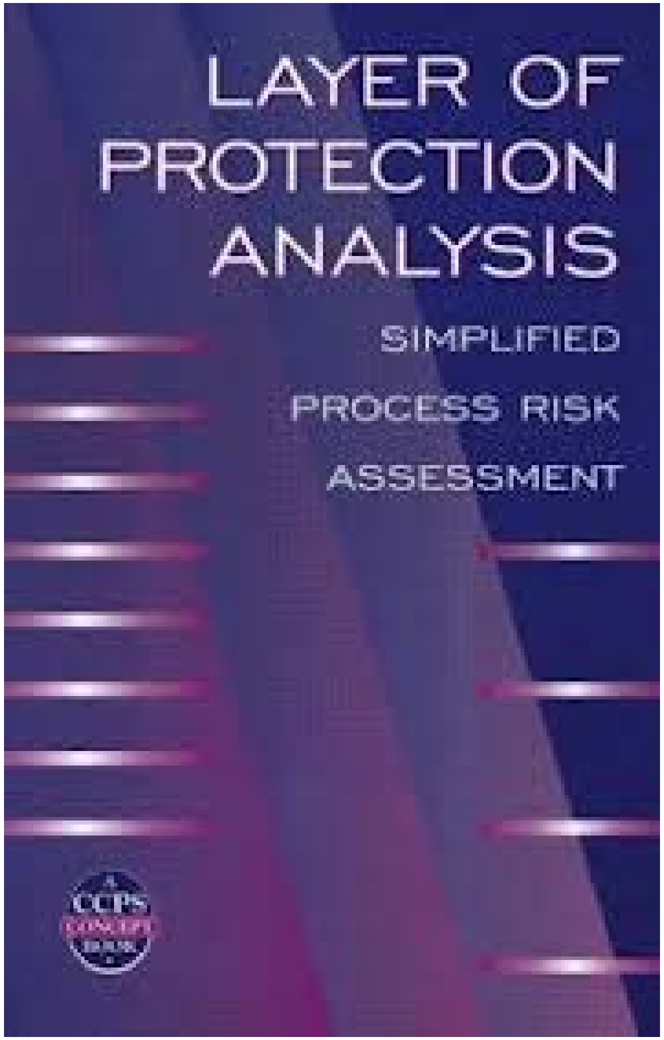
Second Edition

AIChE

CCPS

Layer of Protection Analysis

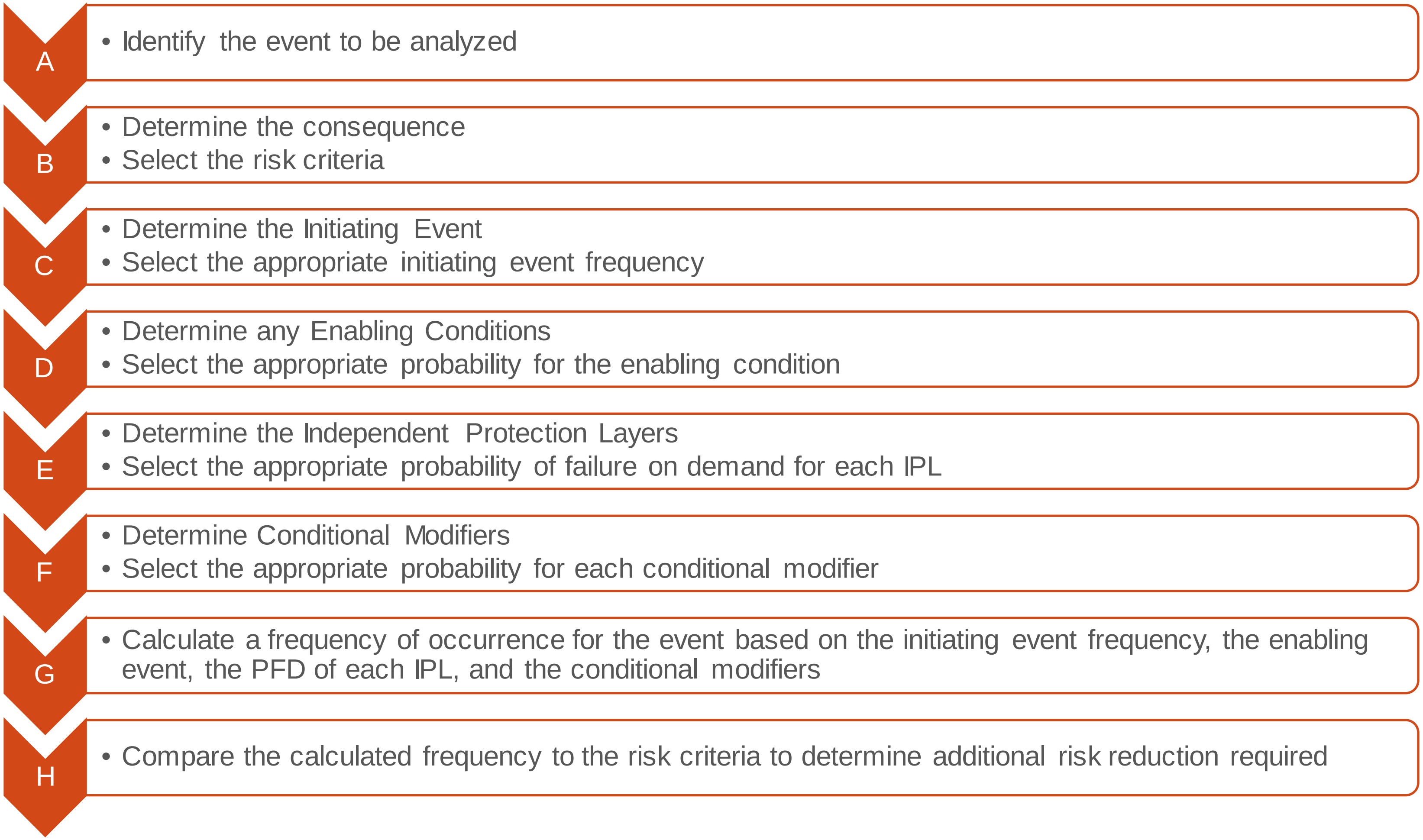
- Introduced in 2001
- Simplified
- Single Cause – Consequence Analysis
- Order of Magnitude
- Strict Rules of Independence


LAYER OF PROTECTION ANALYSIS
SIMPLIFIED PROCESS RISK ASSESSMENT
A CCPS CONCEPT BOOK

How is LOPA used?

- Process Hazard Analysis
  - Evaluation of adequacy
- Safety Instrumented Systems
  - Most popular means of determining the Safety Integrity Level
- Relief Device Design
  - Mitigation of relief cases

LOPA Process



A
- Identify the event to be analyzed

B
- Determine the consequence
- Select the risk criteria

C
- Determine the Initiating Event
- Select the appropriate initiating event frequency

D
- Determine any Enabling Conditions
- Select the appropriate probability for the enabling condition

E
- Determine the Independent Protection Layers
- Select the appropriate probability of failure on demand for each IPL

F
- Determine Conditional Modifiers
- Select the appropriate probability for each conditional modifier

G
- Calculate a frequency of occurrence for the event based on the initiating event frequency, the enabling event, the PFD of each IPL, and the conditional modifiers

H
- Compare the calculated frequency to the risk criteria to determine additional risk reduction required

Swiss Cheese Model

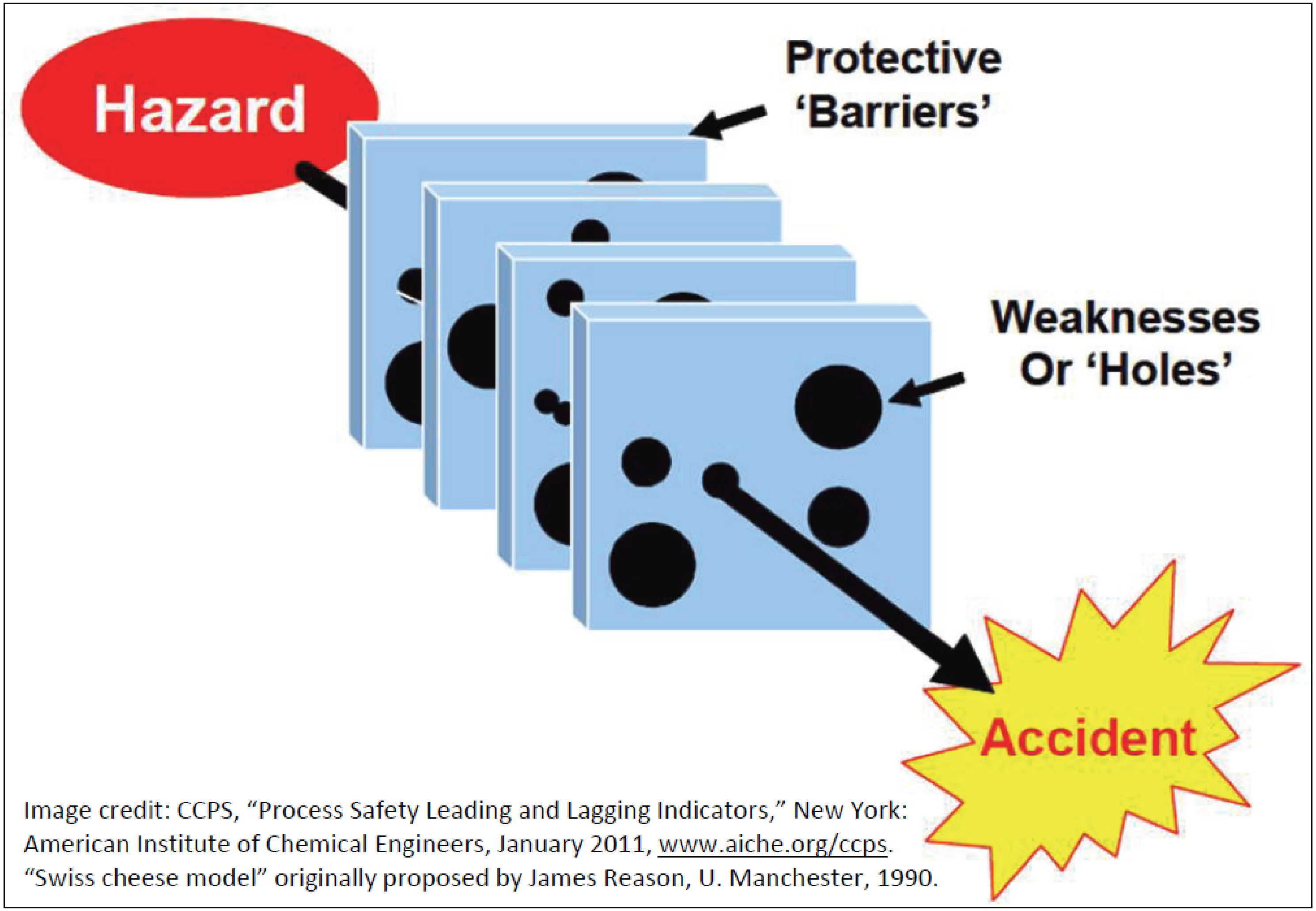


Image credit: CCPS, "Process Safety Leading and Lagging Indicators," New York: American Institute of Chemical Engineers, January 2011, www.aiche.org/ccps. "Swiss cheese model" originally proposed by James Reason, U. Manchester, 1990.

LOPA Process

Determine the Consequence

- The consequence is based on the impact of the event
- Consequence is used to determine the risk criteria
- Loss of primary containment
- Ultimate consequences
  - Life safety
  - Environmental impact
  - Business impact

Initiating Events

- Several initiating events may lead to the consequence of interest
  - Each should be evaluated with an independent LOPA
- Standard values are provided for the initiating event frequencies for most common failures, for example:
  - BPCS (DCS controls) loop failures
  - Operator errors
  - Tube ruptures
  - Loss of cooling

Independent Protection Layers

- IPLs have to meet three basic criteria
  - Independent
  - Effective
  - Auditable
- Standard values are used for the probability of failure on demand (PFD) for IPLs

Conditional Modifiers

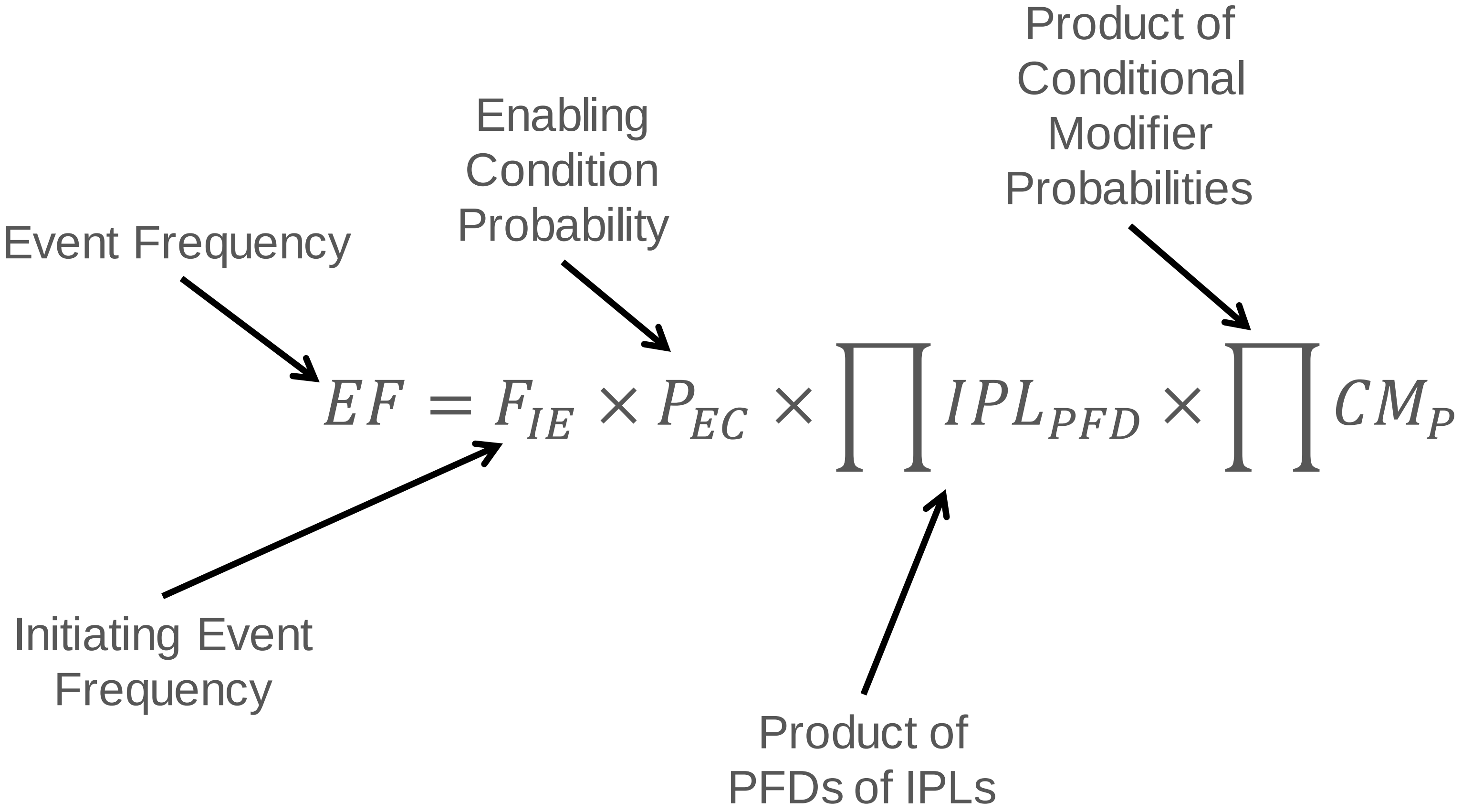
- Probability of Ignition
- Probability of Personnel Presence
- Probability of Injury
- Not typically used if loss of primary containment is the endpoint

Calculated Event Frequency

- The product of the initiating event frequency and the probabilities of the enabling condition, the independent protection layers, and any conditional modifiers provides the calculated event frequency

- The calculated event frequency is then compared to the risk criteria to determine the level of risk and the recommended reliability for additional controls to reduce the risk

Calculated Event Frequency



Product of Conditional Modifier Probabilities

Enabling Condition Probability

Event Frequency

$$EF = F_{IE} \times P_{EC} \times \prod IPL_{PFD} \times \prod CM_P$$

Initiating Event Frequency

Product of PFDs of IPLs

Example LOPA

	Freq. or Prob.	Risk	Description
Scenario			Excessive Steam Flow to Distillation Column Results in Overpressure, Failure, and Severe Injury
Consequence		10^{-5}	Single severe injury on the site
Initiating Event	10^{-1}		BPCS (DCS) Failure of Steam Flow Control
Enabling Condition	1		No enabling condition
IPL	10^{-2}		Relief system design for excessive steam flow
Occupancy	10^{-1}		10% occupancy
Ignition	1		High pressure failure of column (100% ignition probability)
Injury	1		100% probability of injury assumed
Calculated Frequency	10^{-4}		One event in ~10,000 years
Differential		10^{-1}	SIL 1 SIS could be used to address the gap

Consistent Theme

- CCPS has published and continues to publish books related to LOPA
  - Guidelines for Initiating Events and Independent Protection Layers for Layer of Protection Analysis
  - Guidelines for Enabling Conditions and Conditional Modifiers for Layer of Protection Analysis
  - Guidelines for Determining the Probability of Ignition of a Released Flammable Mass
- **Avoiding misuse**

Guidelines for Initiating Events and Independent Protection Layers for Layer of Protection Analysis

Key Changes since LOPA (2001)

- Detailed discussion of each IE and IPL
- Pressure relief systems
- Check valves
- Time dependency
- High demand mode
- BPCS IPLs
- Common cause related to BPCS / SIS layers
- Human factors

Data Sources

- Expert Judgment
- Generic
- Predicted
- Site-Specific

Core Attributes

- Independence
- Functionality
- Integrity
- Reliability
- Auditability
- Access Security
- Management of Change

Initiating Event

Description

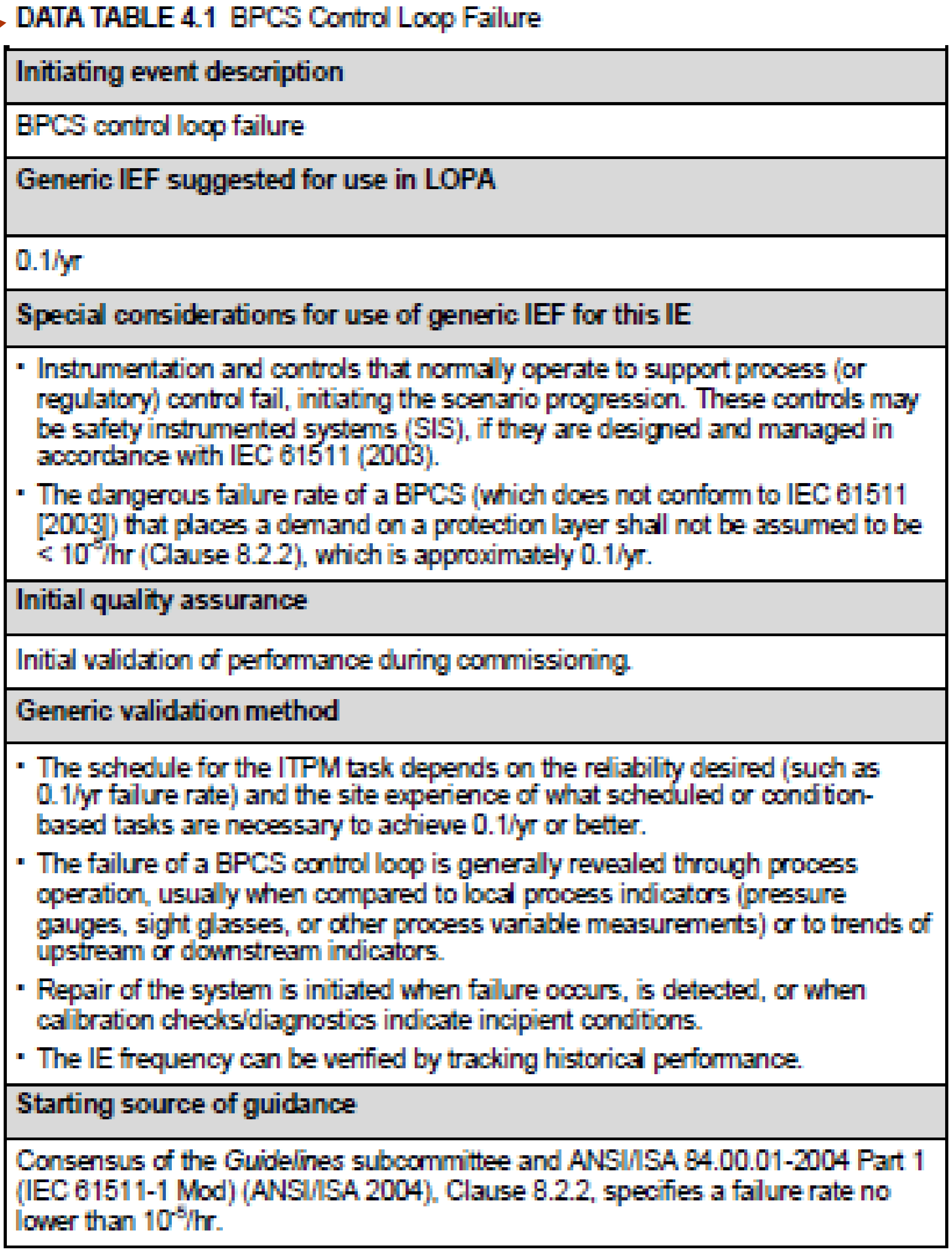
Initiating Event Frequency

Special Considerations

Quality Assurance

Validation

Source of Data



DATA TABLE 4.1 BPCS Control Loop Failure

Initiating event description
BPCS control loop failure
Generic IEF suggested for use in LOPA
0.1/yr
Special considerations for use of generic IEF for this IE
▪ Instrumentation and controls that normally operate to support process (or regulatory) control fail, initiating the scenario progression. These controls may be safety instrumented systems (SIS), if they are designed and managed in accordance with IEC 61511 (2003). ▪ The dangerous failure rate of a BPCS (which does not conform to IEC 61511 [2003]) that places a demand on a protection layer shall not be assumed to be < 10^{-5}/hr (Clause 8.2.2), which is approximately 0.1/yr.
Initial quality assurance
Initial validation of performance during commissioning.
Generic validation method
▪ The schedule for the ITPM task depends on the reliability desired (such as 0.1/yr failure rate) and the site experience of what scheduled or condition-based tasks are necessary to achieve 0.1/yr or better. ▪ The failure of a BPCS control loop is generally revealed through process operation, usually when compared to local process indicators (pressure gauges, sight glasses, or other process variable measurements) or to trends of upstream or downstream indicators. ▪ Repair of the system is initiated when failure occurs, is detected, or when calibration checks/diagnostics indicate incipient conditions. ▪ The IE frequency can be verified by tracking historical performance.
Starting source of guidance
Consensus of the Guidelines subcommittee and ANSI/ISA 84.00.01-2004 Part 1 (IEC 61511-1 Mod) (ANSI/ISA 2004), Clause 8.2.2, specifies a failure rate no lower than 10^{-5}/hr.

Independent Protection Layer

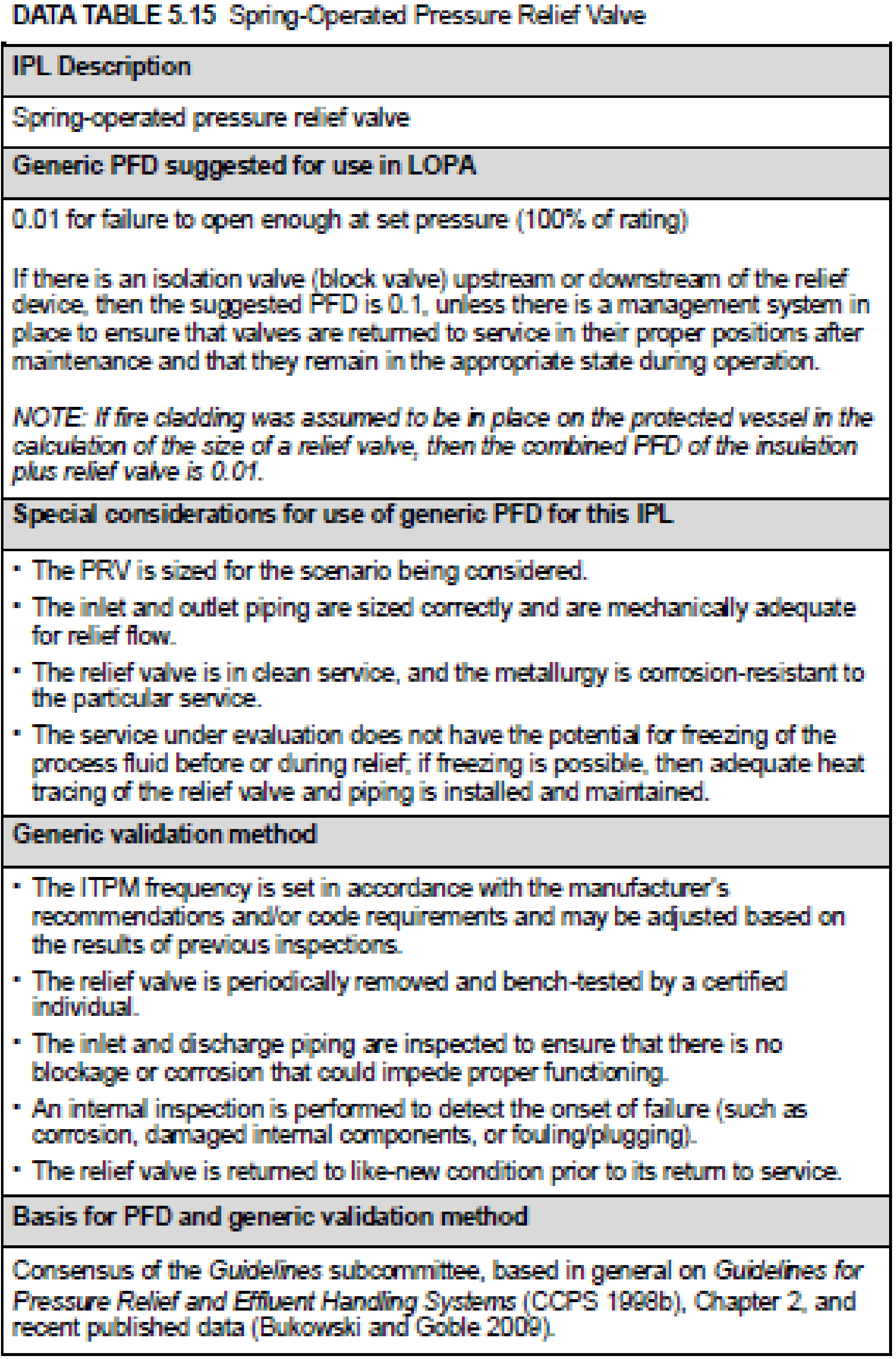
Description

Probability of Failure on Demand
And Notes

Special Considerations

Validation

Source of Data



DATA TABLE 5.15 Spring-Operated Pressure Relief Valve

IPL Description

Spring-operated pressure relief valve

Generic PFD suggested for use in LOPA

0.01 for failure to open enough at set pressure (100% of rating)

If there is an isolation valve (block valve) upstream or downstream of the relief device, then the suggested PFD is 0.1, unless there is a management system in place to ensure that valves are returned to service in their proper positions after maintenance and that they remain in the appropriate state during operation.

NOTE: If fire cladding was assumed to be in place on the protected vessel in the calculation of the size of a relief valve, then the combined PFD of the insulation plus relief valve is 0.01.

Special considerations for use of generic PFD for this IPL

- The PRV is sized for the scenario being considered.
- The inlet and outlet piping are sized correctly and are mechanically adequate for relief flow.
- The relief valve is in clean service, and the metallurgy is corrosion-resistant to the particular service.
- The service under evaluation does not have the potential for freezing of the process fluid before or during relief; if freezing is possible, then adequate heat tracing of the relief valve and piping is installed and maintained.

Generic validation method

- The ITPM frequency is set in accordance with the manufacturer's recommendations and/or code requirements and may be adjusted based on the results of previous inspections.
- The relief valve is periodically removed and bench-tested by a certified individual.
- The inlet and discharge piping are inspected to ensure that there is no blockage or corrosion that could impede proper functioning.
- An internal inspection is performed to detect the onset of failure (such as corrosion, damaged internal components, or fouling/plugging).
- The relief valve is returned to like-new condition prior to its return to service.

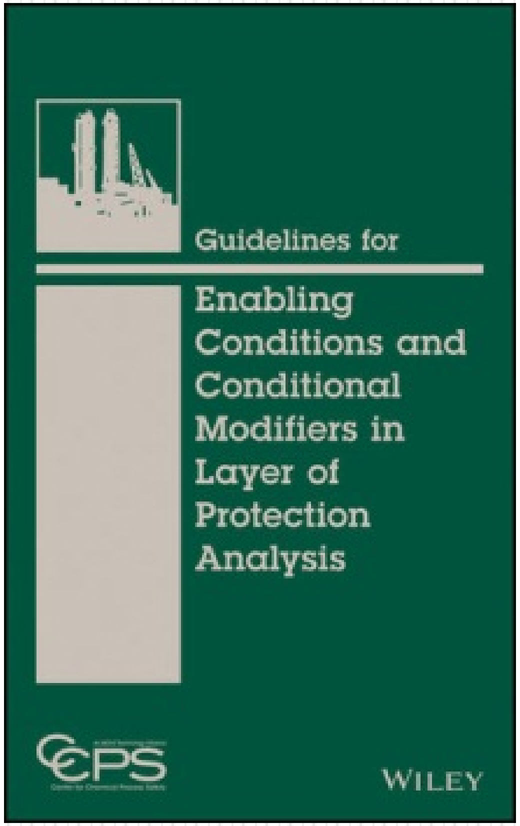
Basis for PFD and generic validation method

Consensus of the *Guidelines* subcommittee, based in general on *Guidelines for Pressure Relief and Effluent Handling Systems* (CCPS 1998b), Chapter 2, and recent published data (Bukowski and Goble 2009).

Advanced Topics

- Utilizing QRA in conjunction with or instead of LOPA
- Use of Human Reliability Analysis in conjunction with LOPA
- Evaluation of complex mitigative IPLs
- Human factors considerations
- Site-specific data collection and validation
- Overpressure of pressure vessels and piping

Guidelines for Enabling Conditions and Conditional Modifiers for Layer of Protection Analysis



Guidelines for

Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis

CCPS

WILEY

Enabling Conditions

- Condition which must be present for an incident sequence to proceed to the consequence of concern
- But is not a failure, error, or a protection layer
- Expressed as a probability

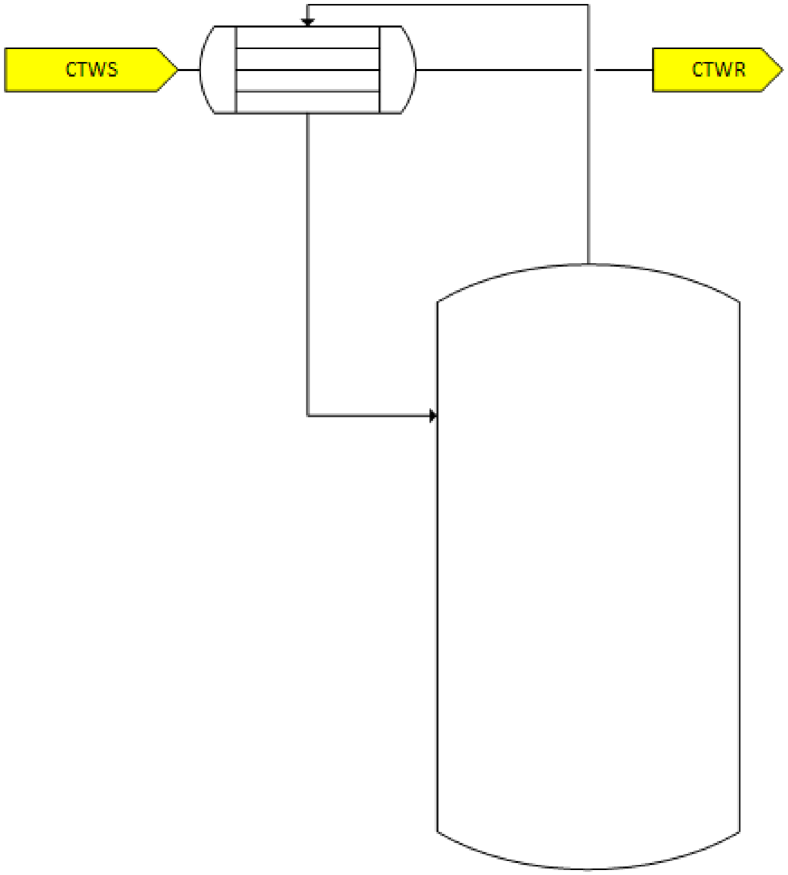
- Should not be used
  - Unless their use is understood by the analyst
  - If insufficient information is available to assess the probability
  - If the company's LOPA procedure does not allow them
  - If the Management of Change process will not capture changes to the probability

Enabling Conditions

- Time-at-risk
  - Seasonal risks
  - Process state risks
- Campaign
  - Facility operated part of the year
  - Facility running several processes

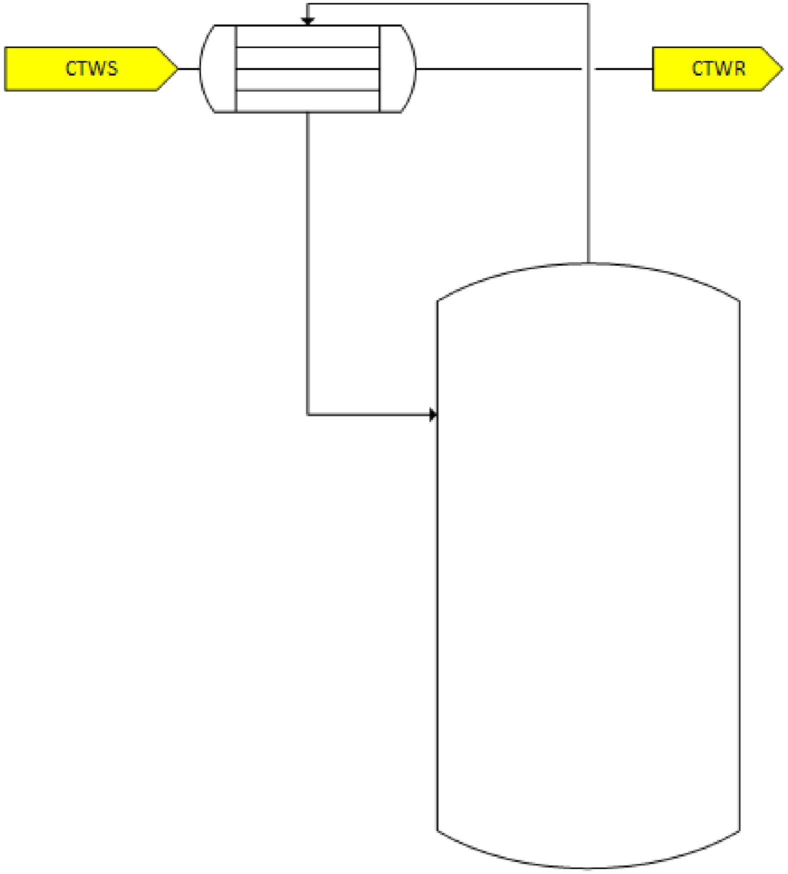
Time-at-Risk Example

- Reaction in a vessel with external condenser to remove heat
- Batch process
- Runaway reaction only possible if cooling is not available during a particular step of the procedure
- Enabling condition?



Time-at-Risk Example

- Enabling condition?
- It depends
- Is the loss of cooling a revealed failure prior to entering the dangerous time-at-risk?



Conditional Modifiers

- Probabilities included in risk calculations
- Risk criteria endpoints are expressed in impact terms instead of loss of containment

- Should not be used
  - If the analyst has insufficient knowledge of conditional modifiers to employ them correctly
  - If they are implicitly included in consequence severity selection
  - If the uncertainty or complexity is deemed to be too great
  - If validation is considered too onerous
  - If a conservative approach is taken
  - If the Management of Change process will not capture changes to the probability

Conditional Modifiers

- Probability of hazardous atmosphere
- Probability of ignition or initiation
- Probability of explosion
- Probability of personnel presence
- Probability of injury or fatality
- Probability of equipment damage or other financial impact

Probability of Personnel Presence

- Must be used carefully if used in conjunction with probability of injury
- Additional detail may be required from consequence assessment
- Must account for all personnel
- Must account for common cause with the event

Pitfalls of Conditional Modifiers

- Not independent of consequence estimate, initiating event, IPLs, or other conditional modifiers
- Using more than are warranted
- Being overly optimistic in estimating values
- Matching risk criteria to their use

Evergreen LOPA Database

Evergreen LOPA Database

- Vision is to provide up to date information on the factors used in LOPA
  - Online
  - Easily accessible
  - Maintained
  - Validated
  - Open to input from the broader community
  - FAQ
- In the current conception, what it will not be:
  - LOPA Wiki
  - Message board or discussion list

Conclusions

- LOPA is an important technique across the chemical industry
- Significant amounts of new information / guidance are available
- Practitioners should be aware of developments in the guidance for the technique and the new and changing standards

Questions?