Inherent Safety and Inherently Safer Reactions

Prof. Attilio Citterio
Dipartimento CMIC “Giulio Natta”
http://iscamap.chem.polimi.it/citterio/education/course-topics/
Risk Assessment Approach

Select focus of the analysis:
- Human;
- Productivity;
- Asset damage;
- Environmental;

Physical effects depend upon Hazard and process conditions;

From physical effects to impact on targets;

From release frequency to outcome frequency (interaction with consequence assessment);

Risk is a function of Likelihood and Magnitude.

Risk = Likelihood × Magnitude
Causes of Losses in Large Plant Accidents

- Mechanical: 44%
- Operator Error: 22%
- Unknown: 12%
- Process upsets: 11%
- Natural Hazards: 5%
- Design: 5%
- Sabotage and arson: 1%
Concept of Safety

- The elimination of accidents (and serious incidents) is unachievable.
- Failures will occur, in spite of the most accomplished prevention efforts.
- No human endeavour or human-made system can be free from risk and error.
- Controlled risk and error is acceptable in an inherently safe system.

Safety is the state in which the risk of harm to persons or property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and risk management.
The Evolution of Safety Thinking

- **1950**: Identify Safety Hazard
- **1970**: Implement Remedial Action to Maintain Safety Performance
- **1990**: Continuously monitor and addresses safety performance of the organization
- **2010**: Seek continuous improvement in the overall performance of the SMS

**Factors**

- **Technical Factors**: Mechanical, improvements, technology
- **Human Factors**: CRM, MRM, Human Performance
- **Organizational Factors**: Continuously monitor and addresses safety performance of the organization

**Today**: SMS

Identify Safety Hazard

Implement Remedial Action to Maintain Safety Performance

Continuously monitor and addresses safety performance of the organization

Seek continuous improvement in the overall performance of the SMS
Inherent Safety (Previous and Recent Strategies)

Pre-1930’s Identify who caused the loss and punish the guilty
Pre-1970’s Find breakdown in, and fix man-machine interface (Trevor Kletz)
1970’s, 80’s Develop risk assessment techniques and systematic approaches
1980’s Performances, risk based standards; regulations
2000’s ‘green’ and ‘inherent safety’ design
2000's Safety Management Systems Complete (SMS-C)

CJChE, vol 81, pp. 2-16 (2003); * ICAO Safety Management manual (2010)
The Management Dilemma

Management levels

Resources

Protection

Production

Resources
Conflicts and Compromises

The properties of a technology that makes it dangerous can be the same which makes it useful:

- Airplanes travel at 960 km·h\(^{-1}\)
- Gasoline is flammable (substitute must be able to stock a big quantity of energy in a compact form)

the danger control is a critical problem in obtaining safely the benefits of technology.

Everything presents multiple dangers:

- Travel in car
  - speed (energy), flammable fuel, toxicity of exhaust gases, hot surfaces, pressurized cooling systems, electricity ......
- Chemical process or product
  - Acute toxicity, flammability, corrosivity, chronic toxicity, various environmental impacts, reactivity ......
What means Inherently Safer Design?

- **Inherent** - “existing in something as a permanent and inseparable element…”
  - safety “built in”, not “added on”
- Eliminate/minimize process hazards than control them
- Three parts:
  - Hazard Identification,
  - Hazard Evaluation and
  - Inherent Safety Evolution
- More a Philosophy and way of thinking than a specific set of tools and methods
  - Applicable at all levels of design and operation from conceptual design to plant operations
- “**Safer**”, not “**Safe**”
Inherently Safer Design, Green Chemistry, and Green Engineering

Inherently Safer Design

Green Chemistry and Engineering
Risk Level in Same Sectors

- Amateur Systems
  - Himalaya climbing
  - Medical Risk (total)
- Sure Systems
  - Process Chemical Industry
  - Charter fly
  - Route Safety
- Ultra-sure Systems
  - Civil Aviation
  - Rails (France)
  - Nuclear Industry

(from R. Amalberti)
Control Systems in Aircraft Industry

- Operation of aircraft
- Maintenance of aircraft
- Air traffic services
- Aerodromes

- Two audience groups
  - States
  - Service providers

- Three distinct requirements
  - Safety programme
  - SMS
  - Management accountability
Strategies – Levels of Intervention and Tools

Baseline performance

Operational performance

Safety management levels

Desirable management level

Highly efficient

Very efficient

Efficient

Insufficient

Hazard

Predictive

Proactive

Reactive

APA

Surveys

Audits

MOR

Accident and incident reports

“Practical drift”
Risk Mitigation at a Glance

Hazard identification and risk management

Assessment of the defenses within the safety system

Control and mitigation of the risk(s)

Accepting the mitigation of the risk

- Does the mitigation address the hazard?
- Does it address the risk(s)?
- Is it effective?
- Is it appropriate?
- Is additional or different mitigation warranted?
- Do the mitigation strategies generate additional risk(s)

Feedback (Safety assurance)
Hazard and Risk

- A **Hazard** is defined as an inherent physical or chemical characteristic that has the potential for causing harm to people, the environment or property. (CCPS, 1992).
- **Hazards** are characteristic of the materials and chemistry.
- **Hazards** are characteristic of the process variables.

Chemical process plants have an inherent risk. Managers of each site must decide what is a tolerable risk. Risk can be reduced by reducing the consequence and/or reducing the probability.

**Examples**
- Phosgene – toxic by inhalation; Acetone - flammable
- High pressure steam - potential energy due to pressure and high temperature

\[
\text{Risk of an Event} = \text{Consequence} \times \text{Probability}
\]
<table>
<thead>
<tr>
<th><strong>Occupational Health and Safety</strong></th>
<th><strong>Process Safety</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Workplace rules</td>
<td>Collective commitment</td>
</tr>
<tr>
<td>Worker training</td>
<td>Addresses events over which the individual worker often has little or no control</td>
</tr>
<tr>
<td>Supervision</td>
<td>Focus on systems</td>
</tr>
<tr>
<td>Individual behaviors</td>
<td>Broader impact – events that could affect groups of workers or general public</td>
</tr>
<tr>
<td>Safety equipment, PPE</td>
<td></td>
</tr>
<tr>
<td>Focus on individual well being</td>
<td></td>
</tr>
</tbody>
</table>

**Objective:** to eliminate injuries and illnesses to personnel, and to protect assets, production, and the environment.

Process Safety is the use of engineering and management competence focused on preventing catastrophic accidents, in particular explosions, fires, and toxic releases, associated with the use of chemicals and petroleum products.
## Risk Based Process Safety

**Commit to Process Safety**
- Process Safety Culture
- Compliance with Standards
- Process Safety Competency
- Workforce Involvement
- Stakeholder Outreach

**Understand Hazards and Risk**
- Process Knowledge Management
- Hazard Identification and Risk Analysis

**Manage Risk**
- Operating Procedures
- Safe Work Practices
- Asset Integrity and Reliability
- Contractor Management
- Training and Performance Assurance
- Management of Change
- Operational Readiness
- Conduct of Operations
- Emergency Management

**Learn from Experience**
- Incident Investigation
- Measurement and Metrics
- Auditing
- Management Review and Continuous Improvement
Risk-based thinking
QMS Structure Re-organized

4. **Context of Organization** – addresses needs and expectations of interested parties, scope of QMS

5. **Leadership** – addresses management commitment, policy, roles, responsibility & authority

6. **Planning** – includes risks, opportunities, objectives and plans to achieve them, the planning of changes

7. **Support** – includes resources, competence, awareness, communication, documented information

8. **Operation** – includes planning & control, determine market needs, interaction w/customers, planning process, control of external provisions of goods/services, production of goods, provision of services, release of goods/services, non-conforming goods/services

9. **Performance Evaluation** – includes monitoring, measurement, analysis & evaluation, internal audit, management review

10. **Improvement** – addresses non-conformity & corrective action, improvement
Certified organizations will have a transition period of three years starting from September 2015 to update their Quality Management Systems to new requirements.
Four Phases of Risk

Risk Analysis
- INTENDED USE Identification
- HAZARD identification
- RISK estimation

Risk Evaluation
- RISK acceptability decisions

Risk Control
- OPTION analysis
- Implementation of measures
- RESIDUAL RISK evaluation
- Overall RISK acceptance

Post Production Information
- Post-production experience
- Review of RISK MANAGEMENT experience - customer use
- Take appropriate actions
Analyse process according to ESARR 4 and standards for risk management.

Documentation:
- FHA
- PSSA
- SSA
- Safety Case
Risk Evaluation

Methods (SAM):
- Hazop
- FMECA
- FTA
- ETA
- Reliability

Risk-informed MTO approach
**Acronyms**

SAM = Safety Assessment Methodologies  
HAZOP = HAZard and OPerability analysis  
FTA = Fault tree analysis, o analisi dell'albero dei guasti  
ETA = Event Tree Analysis  
FMEA = Failure Mode and Effect Analysis  
FMECA = Failure Mode, Effects, and Criticality Analysis  
MTO = Man-Technique-Organisation  
FHA = Functional Hazard Assessment  
PSSA = Preliminary System Safety Assessment  
SSA = System Safety Assessment  
ESARR 4 = EUROCONTROL Safety Regulatory Requirement  
CPPs = Critical Control Points  
QMS = Quality Management Systems
Hazard Identification

Hazard Identification

Hazard identification

- Interaction with third parties
- Natural events

Hazard identification

- Process deviations

Hazard identification

- Corrosion and Material defects,
- Fabrication errors, etc.

Early identification of project Hazard

Guidelines and principles for HAZOP

HAZOP

Project improvement

HAZOP FMECA

Detailed and quantitative analysis to improve project safety

Statistical analysis
Hazard Identification

Release

Pressurized
- Gas
- 2-phase / Liquid
  - Continuous release
  - Flash / Spray
  - Rainout
  - Evaporation

Unpressurized
- Jet
  - Early ignition
  - Late ignition
  - Gas dispersion
  - VCE
  - Pool fire

Other
- External fire
- Cond. phase
- Jet fire
- Flash fire
- Toxic disper.
- Pool fire
- Bleve
- RPT
FMEA PROCESS

- List ALL possible failures
- Classification and quantification (1 to 10) of failures based on:
  - Frequency (F) / probability of failure occurs
  -Severity (S) of the effect
  -Detection (D) of the failure (capacity to detect)
- Prioritization by calculating Risk Priority Number: \[ RPN = F \times S \times D \]
FMEA Metrics

- Fishbone diagram per unit operation to structure process parameters
- A 5 level scale is used to rank the parameters to calculate the Risk Priority Number RPN = I × D × P
- A threshold is settled
- Any value above the setting was studied within a DoE
- Severity/Impact threshold can be added as additional requirement
- Critically is dependent on risk: P×I

<table>
<thead>
<tr>
<th></th>
<th>Impact</th>
<th>Detectability</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>negligible</td>
<td>very high</td>
<td>extremely unlikely</td>
</tr>
<tr>
<td>2</td>
<td>marginal</td>
<td>high</td>
<td>remote</td>
</tr>
<tr>
<td>3</td>
<td>moderate</td>
<td>moderate</td>
<td>occasional</td>
</tr>
<tr>
<td>4</td>
<td>major</td>
<td>low</td>
<td>probable</td>
</tr>
<tr>
<td>5</td>
<td>Critical (unknown)</td>
<td>Very low</td>
<td>frequent</td>
</tr>
</tbody>
</table>
Risk Acceptability

- National/international decision – level of an acceptable loss (ethical, political and economic)

*Risk Analysis Evaluation:*

**ALARP** – as low as reasonable practical (UK, USA)
  “Societal risk has to be examined when there is a possibility of a catastrophe involving a large number of casualties”

**GAMAB** – Globalement Au Moins Aussi Bon = not greater than before (France)
  “All new systems must offer a level of risk globally at least as good as the one offered by any equivalent existing system”

**MEM** – minimum endogenous mortality
  “Hazard due to a new system would not significantly augment the figure of the minimum endogenous mortality for an individual”
**Risk Acceptability**

**Tolerable hazard rate (THR)** – A hazard rate which guarantees that the resulting risk does not exceed a target individual risk

<table>
<thead>
<tr>
<th>SIL</th>
<th>$\text{PFD}_{\text{avr}}$</th>
<th>Risk Reduction</th>
<th>Availability (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$10^{-4}$ to $10^{-5}$</td>
<td>10,000 to 100,000</td>
<td>99.99 to 99.999</td>
</tr>
<tr>
<td>3</td>
<td>$10^{-3}$ to $10^{-4}$</td>
<td>1,000 to 10,000</td>
<td>99.9 to 99.99</td>
</tr>
<tr>
<td>2</td>
<td>$10^{-2}$ to $10^{-3}$</td>
<td>100 to 1,000</td>
<td>99 to 99.9</td>
</tr>
<tr>
<td>1</td>
<td>$10^{-1}$ to $10^{-2}$</td>
<td>10 to 100</td>
<td>90 to 99</td>
</tr>
</tbody>
</table>

$\text{PFD}_{\text{ave}}$ = average probability of failure on demand

Potential Loss of Life (PLL) expected number of casualties per year
Assessing Risk

- Identify Potential Risks
  - Begin with a HAZOP

- Assess Potential Risk Likelihood
  - Equipment failure
  - Human error

- Assess Potential Risk Consequences
  - Impact of an event
Health Hazards

- **Category A - Biological Agents**
- **Category B - Physical Agents**
- **Category C - Chemical Agents**

(only this last section analyzed)
Chemical Hazard

Physical hazard

Reactive chemicals
- Water reactive
- Exploresives
- Fire hazard
- Pyrophoric
- Oxidizer
- Flammables
- Combustible

Health hazard

Target-organ chemicals
- Sensitizers
- Reproductive hazard
- Mutagens
- Carcinogens

Health hazard

Corrosives
- Irritants
- Teratogens

Corrosives
- Oxidizer
- Combustible
- Combustible

Target-organ chemicals
- Sensitizers
- Reproductive hazard
- Mutagens
- Teratogens

Chemical hazard

Health hazard

Reactive chemicals
- Water reactive
- Unstable
- Explosives

Physical hazard

Corrosives
- Irritants
- Carcinogens

Reactive chemicals
- Pyrophoric
- Oxidizer
- Flammables
- Combustible

Explosives

Mutagens

Irritants

Unstable

Teratogens
Chemical Health Effects

- **Irritants**: Inflame skin tissue on contact.
- **Corrosives**: Destroy skin tissue at point of contact.
- **Sensitizers**: Cause allergic reactions.
- **Target-Organ Chemicals**: Damage specific body organs and systems.
- **Reproductive Hazards**: Change genetic information in egg or sperm cells and/or damage fetus after conception.
- **Carcinogens**: Cause cancer.
Examples of Hazard

Chlorine is toxic by inhalation
Sulfuric acid is extremely corrosive to the skin
Ethylene is flammable
High pressure confined steam contains pV energy
Styrene can polymerize releasing heat
Nuclear material is contains chronic toxicity
Large mass at high temperature is an energy source

Toxic, Flammable, Temperature, Pressure
Representative List of Types of Hazards

Fires
- Flash fires
- Pool fires
- Jet fires

Explosions
- Vapor clouds
- Confined deflagrations
- Detonations
- Pressure Vessel Ruptures
  - Runaway Reactions
  - Overpressure
  - Brittle fracture
  - Polymerizations
  - Decomposition
  - Contamination reactions
  - Boiling liquid, expanding vapor

Toxicity
- Environmentally
  - Chronic
  - Acute
  - Individually toxic
  - Broadly toxic
- Pesticides
- Fungicides
- Herbicides
- Insecticides
- Fumigants

Product
- Customer injury
- Waste disposal
<table>
<thead>
<tr>
<th>Molecular Grouping</th>
<th>Toxicity and Fire</th>
<th>Toxicity</th>
<th>Fire and Explosion</th>
<th>Explosion</th>
<th>Environmental</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ammonia</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chlorinated hydrocarbons</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyano compounds</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-bond hydrocarbons</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Epoxides</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hydrides and Hydrogen</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metal acetylides</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nitrogen compounds</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oxygenated compounds of halogens</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oxygenated manganese compounds</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peroxides</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polychlorinated byphenyls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poly-cyclic aromatic hydrocarbons</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>B</td>
<td>Hazardous Event</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------</td>
<td>----------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acids</td>
<td>Chlorates</td>
<td>Spontaneous Ignition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chlorites</td>
<td>Spontaneous Ignition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hypochlorites</td>
<td>Spontaneous Ignition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cyanides</td>
<td>Toxic/Flam Gas</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fluorides</td>
<td>Toxic Gas</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Combustibles</td>
<td>Oxidizers</td>
<td>Heat/Polymerization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anhydrous Chromic Acid</td>
<td>Spontaneous Ignition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Potassium Permanganate</td>
<td>Spontaneous Ignition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sodium Peroxide</td>
<td>Spontaneous Ignition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alkali</td>
<td>Nitro Compounds</td>
<td>Easy to Ignite</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nitroso Compounds</td>
<td>Easy to Ignite</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Reactive Combinations of Chemicals

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>Hazardous Event</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ammonium</strong></td>
<td>Chlorates</td>
<td><strong>Explosive Salts</strong></td>
</tr>
<tr>
<td><strong>Salts</strong></td>
<td>Nitrates</td>
<td><strong>Explosive Salts</strong></td>
</tr>
<tr>
<td><strong>Alkali Metals</strong></td>
<td>Alcohols</td>
<td><strong>Flammable Gas</strong></td>
</tr>
<tr>
<td>Glycols</td>
<td></td>
<td><strong>Flammable Gas</strong></td>
</tr>
<tr>
<td>Amides</td>
<td></td>
<td><strong>Flammable Gas</strong></td>
</tr>
<tr>
<td>Amines</td>
<td></td>
<td><strong>Flammable Gas</strong></td>
</tr>
<tr>
<td>Azo Compounds</td>
<td></td>
<td><strong>Flammable Gas</strong></td>
</tr>
<tr>
<td>Diazo Compounds</td>
<td></td>
<td><strong>Flammable Gas</strong></td>
</tr>
<tr>
<td>Inorganic Sulfide</td>
<td>Water</td>
<td><strong>Toxic/Flam Gas</strong></td>
</tr>
<tr>
<td>Metals</td>
<td>Explosives</td>
<td><strong>Heat/Explosion</strong></td>
</tr>
<tr>
<td>Polymerizable</td>
<td></td>
<td><strong>Polymerization</strong></td>
</tr>
<tr>
<td>Compounds</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Relevant Chemical Accidents or Blasts

<table>
<thead>
<tr>
<th>PLACE</th>
<th>DATE</th>
<th>CHEMICAL</th>
<th>ESTIMATED AMOUNT</th>
<th>CASUALTIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oppau/Ludwigshafen</td>
<td>September 21, 1921</td>
<td>ammonium sulfate, ammonium nitrate</td>
<td>4,500 t exploded</td>
<td>ca. 550 + 50 dead, 1,500 injured</td>
</tr>
<tr>
<td>Flixborough</td>
<td>June 1, 1974</td>
<td>cyclohexane</td>
<td>400 ton inventory, 40 ton escaped</td>
<td>28 dead, 36 + 53 injured</td>
</tr>
<tr>
<td>Beek</td>
<td>November 7, 1975</td>
<td>(mainly) propylene</td>
<td>&gt; 10,000 m³ inventory, 5.5 ton escaped</td>
<td>14 dead, 104 + 3 injured</td>
</tr>
<tr>
<td>Seveso</td>
<td>July 10, 1976</td>
<td>2,4,5-trichlorophenol, dioxin</td>
<td>7 ton inventory, 3 ton escaped</td>
<td>no direct casualties, ca. 37,000 people exposed</td>
</tr>
<tr>
<td>San Juan, Mexico City</td>
<td>November 19, 1984</td>
<td>LPG</td>
<td>&gt; 10,000 m³ inventory</td>
<td>5 + ca. 500 dead, 2 + 7000 injured (mainly outside the plant)</td>
</tr>
<tr>
<td>Bhopal</td>
<td>December 3, 1984</td>
<td>methyl isocyanate</td>
<td>41 ton released</td>
<td>3,800 dead, 2,720 permanently disabled</td>
</tr>
<tr>
<td>Pasadena</td>
<td>October 23, 1989</td>
<td>ethylene, isobutane, hexene, hydrogen</td>
<td>33 ton escaped</td>
<td>23 dead, 130-300 injured</td>
</tr>
<tr>
<td>Toulouse</td>
<td>September 21, 2001</td>
<td>ammonium nitrate</td>
<td>200-300 ton</td>
<td>31 dead, 2442 injured</td>
</tr>
<tr>
<td>Tianjin</td>
<td>12 August 2015</td>
<td>Sodium cyanide and ammonium nitrate</td>
<td>300 ton (NaCN) and 800 ton (NH₄NO₃)</td>
<td>114 dead, 720 injured</td>
</tr>
</tbody>
</table>
Accident Sequence

Initiation  The event that starts the accident
Propagation  The events that maintain/expand the accident
Termination  The events that stop or diminish the accident

The goal of Loss Prevention is:
Minimize the probability that the accident begins.
Maximize the probability that the sequence terminates benignly if it does start.
Minimize the consequence if it terminates malignantly.

Inherently safer strategies can impact the accident process at any of these three stages.
Attilio Citterio

Reduce Inherent Hazards and Improve Protection Layers

→ **Hazard**
  Material or energy - inherent in material or chemistry
  Process variable - how chemistry works in the process

→ **Layers of Protection**
  Passive
  Active
  Procedural

→ **Receptors**
  Process
  Nearby process
  Workers
  Nearby workers
  Public
  Environmental

Reduce or eliminate inherent hazard

Improve inherent protection capability

Gives reduced risk
Prevention/Mitigation and Inherent Safety
*(Typical Layers of Protection - Onion Model)*
The above are the eleven aspects of the API 750 Recommended Practice. This has been adopted in a similar form by OSHA. The above requires significant investment in time, equipment and effort. The object is to reduce Risk given that a Hazard exists. These topics are covered in Plant & Environmental Safety. We are interested in reducing the need for the above by invoking Inherently Safer Processes.
Traditional Risk Management

Consider the following factors:

- Capital cost of safety and environmental equipment
- Capital cost of passive barriers
- Operating and maintenance cost
- Increased maintenance cost for safety instruments
- Increase maintenance for process equipment due to safety requirements
- Operator safety training costs for hazardous materials or processes
- Regulatory costs
- Insurance costs
- Potential property damage, product loss, and business interruption costs if an incident occurs
- Potential liability.
The layers of protection are expensive to build and maintain.

*Capital, Operating, Safety Training, Maintenance, Diversion*

The hazard remains.

*Some combination of failures of the layers of protection will result in an accident.*

Accidents can occur by mechanisms that were unanticipated.

*The hazard remains. Unanticipated mechanisms may not be protected against.*
‘A chemical manufacturing process is **INHERENTLY SAFER** if it reduces or eliminates the hazards associated with materials and operations used in the process, and this reduction or elimination is permanent and inseparable.’
Strategies for Reducing Risk

INHERENT  Eliminating the hazard by using materials and process conditions which are nonhazardous

PASSIVE  Minimizing the hazard by process equipment design features which reduce either the probability or consequence of the hazard without active functioning

ACTIVE  Using controls, safety interlocks, and emergency shutdown systems to detect and correct process deviations (engineering controls)

PROCEDURAL  Using operating procedures, administrative checks, emergency response, and other management approaches to prevent incidents, or to minimize the consequences (administrative controls)

*Presented in order of reliability!*
Strategies for Reducing Risk in Chemical Process – Examples - Inherency

- Eliminate or reduce the hazard by changing to a process or materials which are non-hazardous or less hazardous
- Integral to the product, process, or plant - cannot be easily defeated or changed without fundamentally altering the process or plant design

**EXAMPLES**

- Substituting water for a flammable solvent (latex paints compared to oil base paints)
- An atmospheric pressure reaction using nonvolatile solvents. (No potential for overpressure).
Minimize hazard using process or equipment design features which reduce frequency or consequence without the active functioning of any device

**EXAMPLES**

- Containment dike around a hazardous material storage tank
- A reaction capable of generating 10 atm pressure in case of a runaway in a vessel designed for 20 atm. (The reactor can contain the accident unless e.g. damage).
- Arrange an expansion room to collect gases and liquids originated from possible failures.
Strategies for Reducing Risk in Chemical Process – Examples - Active

- Controls, safety interlocks, automatic shutdown systems
- Multiple active elements
  - Sensors - detect hazardous conditions
  - Logic device – decide what to do
  - Control elements – implement action
- Prevent incidents, or mitigate the consequences of incidents

**EXAMPLE**

- High level alarm in a tank shuts automatic feed valve
- A reaction capable of generating 150 psig pressure in case of a runaway in a 15 psig reactor with a 5 psig interlock that stops feeds and a rupture disk to reduce pressure directing contents to effluent treatment. (What could happen?)

**Caution:** Also protective systems can cause accidents!
Using Standard operating procedures, administrative checks, emergency response, training and other management approaches to prevent incidents, or to minimize the consequences (administrative controls)

**EXAMPLES**

- Confined space entry procedures
- The same reactor as in the previous example without the interlock. The operator is instructed to monitor the pressure and shut down feed. (Human error)
Example: Batch Chemical Reactor

Hazard of concern:

*Runaway reaction causing high temperature and pressure and the potential reactor rupture*

**Passive**

- Maximum adiabatic pressure for reaction determined to be 10 atm
- Run reaction in a 20 atm design reactor
- Hazard (pressure) still exists, but passively contained by the pressure vessel.
Example: Batch Chemical Reactor

Active

- Maximum adiabatic pressure for 100% reaction is 8 atm, the reactor design pressure is 3 atm
- Gradually add limiting reagent with temperature control to limit the potential energy from reaction
- Use high temperature and pressure interlocks to stop feed and apply emergency cooling
- Provide emergency relief systems

Procedural

- The maximum adiabatic pressure for 100% reaction is 8 atm, the design pressure of reactor is 3 atm
- Add gradually the limiting reagent controlling the temperature to limit the potential energy of reaction
- Train operator to observe temperature, stop feeds and apply cooling if temperature exceeds operating limit.
Example: Batch Chemical Reactor

Inherent

- Develop chemistry which is not exothermic, or mildly exothermic
  - Maximum adiabatic exothermic temperature < boiling point of all ingredients and onset temperature of any decomposition or other reactions.

Since Inherently Safer is the most reliable strategy, what are the potential options under inherently safer?
Inherently Safer Processes Strategies

**MINIMIZE**
Use smaller quantities of hazardous materials when the use of such materials cannot be avoided. Perform a hazardous procedure as few times as possible when the procedure is unavoidable. *(Intensification)*

**SUBSTITUTE**
Replace a substance with a less hazardous material or processing route with one that does not involve hazardous material. Replace a hazardous procedure with one that is less hazardous.

**MODERATE**
Use less hazardous conditions, a less hazardous form of a material, or facilities which minimize the impact of a release of hazardous material or energy. Identify processing options that involve less severe processing conditions- *(Attenuation or Limitation)*.

**SIMPLIFY**
Design facilities which eliminate unnecessary complexity and make operating errors less likely, and which are forgiving of errors which are made. *(Error Tolerance)*
When developing a process design, we have typically worried about the robustness in the design specifications and equipment sizes. We want to incorporate safety concerns into our considerations.
Operating Ranges & Limits

- NEVER EXCEED Limit
- Mandatory Action Point
  - Take NEVER DEVIATE to Avoid Consequences
- Quality or Normal Operating Limits
- Safe Operating Limits
  - No consequences
- Instrumentation Range
- Equipment Containment Limits

Set point
Process Risk Management Strategies

Process Risk Management Strategies

- Inherent
- Passive
- Active
- Procedural

Inherently Safer Design Strategies

- Minimize
- Substitute
- Moderate
- Simplify
Inherently Safety in Process Synthesis
(Conceptual Process Design)

The structure that we used during process synthesis is given below. Remember that this isn’t a procedure, it is a decision hierarchy that we follow as the design evolves. Since it is a structure, inherent safety permeates the entire design evolution.

- Process Information
- Process Structure
- Feed, Product, Byproduct & Waste Structure
- Inherent Safety Structure
- Recycle Structure
- Separation Structure
- Heat Integration
- Process Control Structure
### Inherently Safer Design Questions

<table>
<thead>
<tr>
<th>Decision Point</th>
<th>Key Questions</th>
<th>Information Used</th>
</tr>
</thead>
</table>
| Initial Specifications          | What Product?  
What Capacity? | Market Research  
R&D New Product Ideas |
| Process Synthesis Route         | How?  
What Route?  
What Reactions, Materials? | R&D Chemists Research  
Known Synthesis Routes |
| Chemical Flowsheet              | Basis Unit Operation Selection  
Temperatures, Pressures  
Solvents, Catalysts  
Flows, Conversions | Process Synthesis Route  
Laboratory/Pilot Tests  
Existing Process Knowledge |
| Process Flowsheet               | Batch v. Continuous  
Detailed Unit Operations  
Control & Operation Philosophy | Process Engineering Principles |
| Process Conceptual Design       | Equipment, Inventory, Utilities  
Flexibility, Overdesign, Recycles  
Location, Controls, Instrumentation  
Layout, Materials of Construction | Equipment Suppliers Data |
| Process Detailed Design         | Equipment Specification  
Leak Paths, Ease of Control  
Simplify Hazardous Activities | Standards/Procedures Experience |
‘To minimize is to reduce the quantity of material or energy contained in a manufacturing process or plant.’

Reactor Systems
- Understand reaction kinetics
- Use continuous reactors when possible
- Produce and consume hazardous materials in-situ
- Add reactants to a batch reactor continuously

Separation Systems
- Remove hazardous materials early in the distillation sequence
- Use column internals which minimize hold-up and connections
- Evaluate other separation systems which may be safer ($\tau$, inventory)
- Use heat exchangers with minimal area to reduce inventory
‘To minimize is to reduce the quantity of material or energy contained in a manufacturing process or plant.’

**Storage Systems**

- Minimize Storage of hazardous raw materials and intermediates
- Consider ‘just-in-time’ supply
- Reduce pressure driving force (liquids, refrigeration, dilution) to minimize leaks
- Use large particle size, slurries, pastes to minimize dust explosion hazard

*Smaller tanks do little to reduce the hazard when:*
  - *Hazard is primarily from connecting and disconnecting tank trucks or tank cars serving tanks*
  - *Exposure arises from the number of vents, and number and extent of nozzles, valves and lines connecting the tank.*
‘To minimize is to reduce the quantity of material or energy contained in a manufacturing process or plant.’

Piping, etc.
- Design dike drainage so that flammable and combustible materials will not accumulate around tanks
- Minimize surface area of spills of toxic materials with high vapor pressure to minimize vapor released
- Optimize pipeline length by attention to layout
- Pipe size should be sufficient to convey required amount and no more
- Provide proper support especially for small pipe
- Transfer by gas, if possible, instead of liquid
Minimize: Scale-up?

- Minimize
  - Use small quantity of energy or dangerous compounds
  - Storage of raw materials
  - Storage of intermediates
  - Piping
  - Process equipment

"Process Intensification"
(continuous processes)
• Reduced consequences of accidents (explosions, fires, emission of toxic materials) and no production stop.

• Improved efficiency and use of other protection systems

  *for example:*
  • Secondary containment
  • Reactor unloading or extinction systems
Minimization Checklist

- Have all in-process inventories of hazardous materials in storage tanks been eliminated?
- Are all of the proposed in-process storage tanks really needed?
- Has all processing equipment handling hazardous materials been designed to minimize inventory?
- Is process equipment located to minimize length of hazardous material piping?
- Can piping sizes be reduced to minimize inventory?
- Can other types of unit operations or equipment reduce material inventories?
- Is it possible to feed hazardous materials as a gas instead of liquid, to reduce inventories?
- Is it possible to generate hazardous reactants ‘in-situ’ from less hazardous raw materials?
- Is it possible to generate hazardous reactants on site from less hazardous materials, minimizing the need to store or transport large quantities of hazardous materials?
Substitute

‘Substitution means the replacement of a hazardous material or process with an alternative which reduces or eliminates the hazard.’

**Alternative Chemistry**
- Polymerize then halogenate to avoid using hazardous monomers
- Generate and immediately consume the hazardous substance - DuPont v. Union Carbide for carbamate insecticides
- Phase transfer of catalysts

**Alternative Solvents**
- Use water-based solvents v. organic-based
- Use aqueous or dry flowable formulations of agricultural chemicals
- Minimize use of chlorofluorocarbons for cleaning
- Use less toxic solvents in extractive distillation

**Utility Systems**
- Use water or steam for heat transfer
- Use high flashpoint oils or molten salts where steam or water is not feasible
Improvements in Manufacturing Process of Viagra™ (Pfizer)

1300 L/kg Medicinal Chemistry 1990
100 L/kg optimized-MC 1994
22 L/kg Commercial (1997)
7 L/kg Commercial after solvents recovery
4 L/kg Next objective

Methylene Chloride

t-Butanol
Butanone
Ethyl acetate
Toluene

Chemical structure of Viagra™
Inherent safe design-inventory only?
Substitution Checklist

Is it possible to completely eliminate hazardous raw materials, process intermediates, or by-products by using an alternative process or chemistry?

Is it possible to completely eliminate in-process solvents by changing chemistry or processing conditions?

Is it possible to substitute less hazardous raw materials?
  - Noncombustible rather than flammable solvents
  - Less volatile raw materials
  - Less toxic raw materials
  - More stable raw materials

Is it possible to substitute less hazardous final product solvents?

For equipment containing materials which become unstable at elevated temperature or freeze at low temperature, is it possible to use heating and cooling which limit the maximum and minimum temperatures attainable?
’Moderate means using materials under less hazardous conditions.’

**Dilution**
- Dilute to lower vapor pressure
- Dilute to reduce initial release concentration

**Refrigeration**
- Refrigerate to reduce storage pressure
- Refrigerate to reduce initial flash in event of a leak
- Refrigerate to eliminate aerosol formation in event of a leak (reduced driving force, reduced superheat, reduced two phase jet)

**Particle Size**
- Use large particle size to reduce employee exposure
- Use slurry or paste
Moderate means using materials under less hazardous conditions.'

**Operating Conditions**
- Use conditions which reduce temperature
- Use conditions which reduce pressure

**Isolation by Siting/Location**
- Design to reduce the potential of an incident at one operating site initiating an incident at another
- Consider opportunities to eliminate transport of hazardous materials within the plant
Moderate means using materials under less hazardous conditions.’

**Process Deviations**
- Limit rate of material addition by pump sizing and line sizing
- Size charge/feed tanks to prevent overcharging reactants
- Design fill piping/valving to prevent direct charging from storage tanks to the reactor
- Select heat transfer media to limit maximum or minimum attainable reactor temperature

**Storage Tanks**
- Dike properly to reduce consequences of a spill

**Containment Buildings**
- Limit impact of loss of containment for toxic materials
The containment building and small pipe moderates the consequence of a leak, accident or failure.
Moderate Example: Dilution

- Aqueous ammonia instead of anhydrous one
- Aqueous HCl instead of anhydrous HCl
- Sulfuric acid instead of oleum
- Wet benzoyl peroxide instead of the anhydrous one
- Dynamite instead of liquid nitroglycerin
Moderation Checklist

- Can the supply pressure of raw materials be limited to less than the working pressure of the vessels they are delivered to?
- Can reaction conditions (temperature, pressure) be made less severe by using a catalyst or by using a better catalyst?
- Can the process be operated at less severe conditions? If this results in lower yield or conversion, can raw material recycle compensate for this loss?
- Is it possible to dilute hazardous raw materials to reduce the hazard potential?
- Can process units be located to reduce or eliminate adverse impacts from other adjacent hazardous installations?
- Can the plant site be chosen to minimize the need for transportation of hazardous materials and to use safer transport methods and routes?
- Can a multi-step process, where the steps are done at separate sites, be divided up differently to eliminate the need to transport hazardous materials?
‘Simplifies means designing to eliminate unnecessary complexity, reducing the opportunities for error and misoperation.’

**Equipment**
- Design equipment to contain excursion within equipment (min/max)
- Consider a separate vessel for containment and treatment for relief effluent
- Design S&T HEX to contain maximum pressure

**Piping Systems**
- Minimize use of sight glasses, flexible connections, bellows etc.
- Use welded pipe
- Use gaskets less prone to catastrophic failure
- Provide proper support
- Use gravity, pressure and vacuum systems for transfer
- Use seal less pumps
Attilio Citterio

‘Simplifies means designing to eliminate unnecessary complexity, reducing the opportunities for error and misoperation.’

Processing Steps
- Avoid multi-step reactions in a single vessel

Fail Safe Valving
- Specify process valves to fail closed
- Specify cooling valves to fail open
  *Note that in some cases, specify valves to fail in last position*

Control
- Avoid catastrophic failure due to module failure having multiple inputs/outputs

Information
- Avoid information overload on the operators
- Control the number of alarms
- Provide adequate communication
Simplify - Eliminate Equipment

- Reactive distillation methyl acetate process (Eastman Chemical)
- Which is simpler?

Fewer vessels, pumps, flanges, valves, piping, instruments….

But: Reactive distillation column itself is more complex
Multiple unit operations occur within one vessel
More complex to design
More difficult to control and operate
Complex Batch Single Reactor

Diagram showing components such as:
- Large rupture disk
- Condenser
- Distillate receiver
- Refrigerated brine
- Steam
- Water return
- Water supply
- Condensate
This simpler system reduces the opportunity for chemical interactions and utility usage mistakes.

But there are conflicts of inherent safety

- now there are three vessels, the overall plant is somewhat more complex
- Need to understand the specific hazard for each situation to settle which is the best
Can equipment be designed sufficiently strong to totally contain the maximum pressure generated, even if the ‘worst credible event’ occurs?

Is all equipment designed to totally contain the materials which might be present inside at ambient temperature or the maximum attainable process temperature?

Can several process steps be carried out in separate processing vessels rather than a single multipurpose vessel? This reduces complexity and the number of raw materials, utilities and auxiliary equipment connected to a specific vessel, thereby reducing the potential for hazardous interactions.

Can equipment be designed such that it is difficult or impossible to create a potential hazardous situation due to an operating error?
Best Available Techniques (BAT)

Bring together environmental issues and economic viability.

More specifically ….

**Best** = “(…) most effective in achieving a high general level of protection of the environment as a whole.

**Available** = “techniques' (…) developed on a scale which allows implementation in the relevant industrial sector, under economically and technically viable conditions, taking into account the costs and advantages, (……)*

**Techniques** = “(…) both the technology used and the way in the installation is designed, build, maintained, operated and decommissioned.

IPPC directive, article 2

*Consideration to be taken into account when determining Best Available Techniques are listed in the Annex IV of the IPPC directive.
CT and EOPA are included in BAT

- BAT Technologies include both **Clean Technologies AND End of Pipe Approaches**

**Clean Technologies**

- Forward looking, anticipate and prevent approach

**End of pipe approaches**

- After the event, reach and treat approach

**Best Available Techniques**

Since BAT also include End of Pipe Approaches, it is not always the optimal solution from an ecological, economical, and social point of view.
## BAT Measures for Principal Process Units in Tannery

<table>
<thead>
<tr>
<th>PROCESS UNIT</th>
<th>BAT is:</th>
</tr>
</thead>
</table>
| **Curing and soaking**| ● To process fresh hides as far as they are available  
   Exceptions:  
   ● When long transport time is necessary (max 8 - 12 hours for fresh, unchilled hides; 5 – 8 days if a cooling chain of 2°C is maintained)  
   ● For certain types of end-products  
   ● Sheepskins, calf skins  
   ● To reduce the amount of salt used as far as possible. |
| **Unhearing & liming**| ● To use hair-save technology, but economics can be an issue for existing plants when re-use of the saved hair is impossible  
   ● To reduce sulphide consumption by the use of enzyme preparations; not for sheepskins  
   ● To recycle spent liquors only when processing sheepskins, which are dewoolled by painting |
| **Splitting**         | ● To use lime splitting  
   Exceptions:  
   - When the starting material is wet blue  
   - When a firmer leather has to be produced (e.g. shoe-leather)  
   - When a more uniform and accurate thickness is needed in the final product  
   ● To maximise the use of split |
<table>
<thead>
<tr>
<th>PROCESS UNIT</th>
<th>BAT is:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TAN</strong>YARD <strong>OPERATIONS</strong></td>
<td></td>
</tr>
<tr>
<td>Deliming and bating</td>
<td>● To make a partial substitution of ammonium salts with CO₂ and/or weak organic acids</td>
</tr>
</tbody>
</table>
| Sheepskin degreasing        | ● To optimise wet degreasing using surfactants, with or without organic solvents  
● Closed machines with abatement for air and waste water releases when organic solvents are used to degrease skins in dry state |
| Pickling                    | ● To use partial recycling or re-use of pickle liquors  
● To use a volume of floats in the range of 50 – 60% (based on fleshed weight) for ovine skins and bovine hides in order to reduce salt consumption |
| Tanning                     | ● To increase the efficiency of the chrome tanning process through careful control of pH, float, temperature, time and drum speed, all in combination with chrome recovery through precipitation for waste water streams containing C_{\text{total}} > 1 g/l  
● To use high-exhaustion tanning methods where chrome recovery is not possible  
● To maximise exhaustion of the vegetable tanning liquor with counter-current (pit system) or recycling (drum tanning) |
## BAT Measures for Principal Process Units in Tannery

<table>
<thead>
<tr>
<th>PROCESS UNIT</th>
<th>BAT is:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>POST-TANNING OPERATIONS</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Retanning, chrome fixation and neutralization | ● To enhance exhaustion of post-tanning treatment agents and fixation of tanning agents in the leather  
● To reduce the salt content of spent liquors |
| Dyeing | ● To enhance exhaustion of dyestuffs |
| Fat liquoring | ● To enhance exhaustion of fat liquor |
| Drying | ● To optimise mechanical dewatering prior to drying where possible |
| Applying a surface coat | ● To use roller coating  
● To use curtain coating  
● To use HVLP spray guns  
● To use airless spray guns  
Exception for all four above-mentioned techniques:  
● When very thin finishes are applied, e.g. on aniline and aniline-type leather |
Performance Based Terminology

- SIF – Safety Instrumented Function
- SIL – Safety Integrity Level
- SIS – Safety Instrumented System

Failure Modes
- Fail to Safe vs. Fail to Danger
- Fail Detected vs. Fail Undetected

Quantitative Risk Analysis Methods
- LOPA – Layer of Protection Analysis
- Fault Tree
- Markov Models

PFD – Probability of Failure on Demand
Explaining the Terminology

**SIF** is a single function

- **PST** (Initiating Device)
- **Logic Solver (PLC)**
- **SDV** (Output Device)

**SIL** is the strength of the SIF, how reliable does it need to be.

**SIS** is the entire process safety system, but mainly focuses on the logic solver.
Hazard Analysis / Risk Mitigation

- Hazard Analysis / Risk Mitigation requires knowing the chance that something will fail. Either creating a hazard or failing to protect from a hazard.

- Probability of failure on demand (PFD) is required for any type of quantitative risk analysis.

- PFD is the chance that a device will fail in an un-safe manner that places the facility at risk and is based on the failure rate and the test interval.
Reliability vs. Availability

- **Availability** is the percent of time the device is available to operate. *Percentage of time the system works satisfactorily.*

- **Reliability** The likelihood that the system will work satisfactorily over a given period of time and in appropriate circumstances. *(Low PFD)* is usually achieved at the cost of availability.

- To have high reliability and high availability requires voting logic of multiple sensors, logic solvers and output devices.

- Cost of field devices can rapidly escalate the cost of the safety system.
“System comprised of sensors, logic solvers, and final control elements for the purpose of taking a process to a safe state when predetermined conditions are violated.” (As defined in ANSI/ISA 84.00.01)

ex. Transmitters, Logic Solver, & Valves
SIL Calculations

Things to be modeled include:

- **Sensors**: transmitters, switches, intrinsically safe barriers, interposing relays, etc.
- **Logic Solver**: relays, solid state devices, PLC’s, Safety PLC’s, interposing relays, etc.
- **Final Elements**: valves, solenoids, motor starters, interposing relays, intrinsically safe barriers, etc.
Safety Lifecycle

Planning

Front End Engineering

Engineering Design

Commissioning

Operations & Maintenance

Management of Change
Safety Life Cycle – ISA S84.00.01-2004

Analysis
- Conceptual Process Design
- Identify Potential Risks
- Consequence Analysis
- Layer of Protection Analysis
- Develop Non-SIS Layers

Realization
- Select SIS Technology
- Select SIS Architecture
- Determine Test Frequency

Operation
- Startup
- Operation
- Maintenance
- Periodic Proof Tests
- Modifications
- Decommissioning

How much safety do I need?

How much safety do I have with my design?

How will I keep it safe?

Modify?

Yes

No

Modify?

Yes

No

Drawing by Hal Thomas
Safety Lifecycle

- **Start**
- **Conceptual Process Design**
- **Perform Process Hazards Analysis & Risk Assessment**
- **Apply non-SIF protection layers to prevent identified hazards or reduce risk**

**SIF Required?**
- **No**
- **Yes**
  - Define target SIL

**Perform SIF Conceptual Design, & verify it meets the SRS**

**Develop Safety Requirements Specification**

- **Perform SIF Conceptual Design, & verify it meets the SRS**
- **Perform Hardware Safety Fault Tolerance Analysis**
- **Meet Hardware Fault Tolerance**
  - **Yes**
    - **Perform SIF Detail Design**
    - **SIF installation, Commissioning and Pre-Startup Acceptance Test**
  - **No**
    - **Establish Operation & Maintenance Procedures**
    - **Pre-Startup Safety Review (Assessment)**
    - **SIF startup, operation, Maintenance, periodic functional testing**
    - **Modify or Decommission SIS?**
      - **Modify**
      - **Decommission**
      - **SIF Decommissioning**
Performance Based Example

PIC/PCV Failure – $1 \times 10^{-1}$ (events/year)

Result – The inherent risk of over pressuring the vessel is the sum of the causes which is $1.0 \times 10^{-1}$ events/year or 10% chance or an event every 10 years.
Multiple ways to perform analysis exist (Risk Graph, Risk Matrix, Layer of Protection, Quantitative Risk Analysis).
Base Risk of $1.0 \times 10^{-1}$ /year or 10%
Establish Risk Threshold of $1 \times 10^{-5}$ /year or 0.001% chance

Add PSV (PFD $1 \times 10^{-3}$) results in a remaining risk of $1.0 \times 10^{-4}$ /year or 0.01% chance.
Required PFD of the PSH is equal to risk threshold divided by remaining risk = $(1 \times 10^{-5}/1.0 \times 10^{-4}) = 1.0 \times 10^{-1}$
This is a SIL 1 PSH
Safety Instrumented System Standards

IEC 61508 - “Functional Safety: Safety Related Systems”
Current version released 1999
Revision released 2005

Published 2003

ISA 84.01-2003 - “Functional Safety: Safety Instrumented Systems for the Process Industry Sector”
Identical to IEC 61511 with inclusion of grandfather clause
Published October 2003
IEC 61511 Safety Lifecycle Objectives

1. Analyze
   Hazard Analysis / Risk Assessment: Define Design Targets

2. Design
   Execute HW & SW Design

3. Verify
   Evaluate Design: Reliability Analysis of Safety Integrity & Availability

4. Operate & Maintain
   Document

5. Modify
   Document

6. Modify
   Document

7. Modify
   Document

8. Modify
   Document

9. Modify
   Document

10. Modify
    Ok
Attilio Citterio

Realization Phase - SIF Design Process

Safety Requirements Specification - Functional Description of each Safety Instrumented Function, Target SIL, Mitigated Hazards, Process parameters, Logic, Bypass/Maintenance requirements, Response time, etc.

7. SIS Conceptual Design
   7a. Select Technology
   7b. Select Architecture
   7c. Determine Test Philosophy
   7d. Reliability, Safety Evaluation

Choose sensor, logic solver and final element technology
Redundancy: 1oo1, 1oo2, 2oo3, 1oo2D

SIL Achieved?

No

Yes

8. SIS Detailed Design

Manufacturer’s Safety Manual

Manufacturer’s Installation Instructions

Failure Data Database

Failure Data


10. SIS Installation, Commissioning and Pre-startup Acceptance Test

Detailed Design Documentation - Loop Diagrams, Wiring Diagrams, Logic Diagrams, Panel Layout, PLC Programming, Installation Requirements, Commissioning Requirements, etc.

Drawing copyright 2006, exida.com LLC, Safety Lifecycle Poster,
References and sites on Inherently Safer Chemical Reactions

- Inherently Safer Processes [Link](http://www.ems.org/chemical_plants/inherent_safety.html)
- Responsible Care Toolkit: Security Assessment [Link](http://www.responsiblecaretoolkit.com/security_guidance_siteSec.asp)