INHERENT SAFETY IMPLEMENTATION THROUGHOUT THE PROCESS DESIGN LIFECYCLE

Alessandro Tugnoli\textsuperscript{a}, Faisal Khan\textsuperscript{b} & Paul Amyotte\textsuperscript{c}

\textsuperscript{a}Universita degli Studi di Bologna, Bologna, Italy
\textsuperscript{b}Memorial University, St. John’s, Canada
\textsuperscript{c}Dalhousie University, Halifax, Canada
OUTLINE

Introduction
- The Larger Picture (Risk Management Framework)
- Process Design Lifecycle
- Hierarchy of Risk Control Strategies
- Inherent Safety

Design Assistance Method for Inherent Safety Implementation
- Design Space
- Methodology
- Application

Concluding Remarks
INTRODUCTION

Scope
- Enhancement of industrial safety through recognition of the applicability of inherent safety to other risk control strategies and to stages later in the design lifecycle

Motivation
- Protection of people, environment, assets and production
- Provision of a methodology for consideration of inherent safety principles throughout all levels of the hierarchy of risk controls and all stages of the process design lifecycle
**GENERIC FRAMEWORK FOR RISK MANAGEMENT**

- **Planned Reviews**
- **Management Activities**
  - To track company actions against policy.
  - To track, look for and analyze and assess hazards or concerns that arise that challenge policy.
  - To ensure company activities keep risks under control.

**Management Activities**

- **Identification of Hazards**
- **Risk Analysis/Assessment**
- **Reduce the Risk**
- **Can the risk be reduced?**
  - Yes
  - No
- **Is the risk acceptable?**
  - Yes
  - No
- **Discontinue the Activity**
- **Manage the Residual Risk**
Process Design Lifecycle

- Process Research and Development
- Conceptual Design
- Basic Design
- Detailed Design
- Procedure Design
  - Operation
  - Emergency
Hierarchy of Risk Control Strategies

INHERENT SAFETY

PASSIVE ENGINEERED (ADD-ON) SAFETY

ACTIVE ENGINEERED (ADD-ON) SAFETY

PROCEDURAL (ADMINISTRATIVE) SAFETY
Inherent Safety

From dictionary – *inherent*
- Belonging to the very nature of a person or a thing
- Stresses the inseparability of a part, element or quality

Characteristics of a design which prevent hazards or mitigate consequences
- Utilize underlying physics and chemistry

Trevor Kletz:
- *What you don’t have, can’t leak*
Principles of Inherent Safety

Four main principles of inherent safety are:

- Minimization
- Substitution
- Moderation
- Simplification
Principles of Inherent Safety

Minimization:
Minimize amount of hazardous material in use (when use of such materials cannot be avoided – i.e. elimination)
Principles of Inherent Safety

Substitution:
Replace substance with less hazardous material; replace process route with one involving less hazardous materials
Principles of Inherent Safety

Moderation:
Use hazardous materials in least hazardous forms; run process equipment with less severe operating conditions (e.g. T and P)
Principles of Inherent Safety

**Simplification:**
Simplify equipment and processes that are used; avoid complexities; make equipment robust; eliminate opportunities for error
DESIGN ASSISTANCE METHOD FOR INHERENT SAFETY IMPLEMENTATION

Basic concept is rigorous exploration of inherent safety applicability within the Design Space.

Methodology involves series of nested cycles to facilitate systematic analysis through design lifecycle stages, risk control levels, and inherent safety guidewords (principles).

Application should result in an inherent safety-optimized design for each lifecycle stage.
The Design Space

Process Design Lifecycle (lifecycle stages)

- Procedure Design (operation & emergency)
- Detailed Design
- Basic Design
- Conceptual Design
- Process R&D

Inherent Safety (IS guidewords)

- Inherent
- Passive (engineered)
- Active (engineered)
- Procedural

Risk Control Strategy (control levels)

- Simplification
- Moderation
- Substitution
- Minimization
Start lifecycle stage

Hazard identification

Generate a base option

Knowledge bank

Hazards

Safety measures

Start control level

Analysis

Assessment

Interpretation

Improvement (guideword based)

Next IS guideword

No

All IS guidewords for each hazard applied?

Next control level

No

All control levels analyzed?

Next lifecycle stage

No

All lifecycle stages analyzed?

Stop
Simplification
Minimization

Process Design Lifecycle
(lifecycle stages)

Procedure Design
(operation & emergency)
Detailed Design
Basic Design
Conceptual Design
Process R&D

Inherent Safety
(IS guidewords)

Moderation
Substitution
Minimization

Risk Control Strategy
(control levels)

Inherent Passive Active
Passive (engineered) Active (engineered) Procedural
The Design Space

Process Design Lifecycle
(lifecycle stages)

Inherent Safety
(IS guidewords)

Risk Control Strategy
(control levels)

Simplification

Process R&D

Conceptual Design

Basic Design

Detailed Design

Procedure Design
(operation & emergency)

Inherent

Passive (engineered)

Active (engineered)

Procedural

Moderation

Substitution

Minimization
Muster Sequence

Initiating Event $(t_I)$

Time to Muster $(t_M)$

Muster Actions

Awareness Phase $(t_A)$

Egress Phase $(t_{Eg})$

Evaluation Phase $(t_{Ev})$

Elevated Exposure Phases (EEPs)

Recovery Phase $(t_R)$

Abandon or Stand Down

Risk increasing with time to muster
# Muster Actions

<table>
<thead>
<tr>
<th>Awareness Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Detect alarm</td>
</tr>
<tr>
<td>2 Identify alarm</td>
</tr>
<tr>
<td>3 Act accordingly</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Evaluation Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 Ascertain if danger is imminent</td>
</tr>
<tr>
<td>5 Muster if in imminent danger</td>
</tr>
<tr>
<td>6 Return process equipment to safe state</td>
</tr>
<tr>
<td>7 Make work place as safe as possible in limited time</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Egress Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 Listen and follow PA announcements</td>
</tr>
<tr>
<td>9 Evaluate potential egress paths and choose route</td>
</tr>
<tr>
<td>10 Move along egress route</td>
</tr>
<tr>
<td>11 Assess quality of egress route while moving to TSR</td>
</tr>
<tr>
<td>12 Choose alternate route if egress path is not tenable</td>
</tr>
<tr>
<td>13 Collect personal survival suit if in room at time of muster</td>
</tr>
<tr>
<td>14 Assist others if needed or as directed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recovery Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 Register at TSR</td>
</tr>
<tr>
<td>16 Provide pertinent feedback, if any, attained while enroute to TSR</td>
</tr>
<tr>
<td>17 Don personal survival suit or TSR survival suit if instructed to abandon</td>
</tr>
<tr>
<td>18 Follow OIM’s instructions</td>
</tr>
</tbody>
</table>
Awareness Phase Action 1: Alarm Detection for Given Scenario

**Lifecycle Stage:** Detailed Design (for alarm specification)
- Note that choice will impact muster process during procedure design stage

**Hazard Identification:** Errors in alarm detection
- Knowledge bank must include human error
- Knowledge bank must include safety measures such as training, procedures, equipment, etc.

**Base Option:** Industry-standard or previously installed alarm type
Awareness Phase Action 1: Alarm Detection for Given Scenario

- **Initial Control Strategy Level**: Inherent Safety

- **Assessment**: Expert judgment indexing technique to estimate likelihood of alarm detection errors and resultant consequences

- **Interpretation**: Relative importance of alarm detection in overall muster sequence
Awareness Phase Action 1:
Alarm Detection for Given Scenario

- **Improvements:** Application of IS guidewords
  - e.g. *Minimization* (of obstructions near alarms)
  - e.g. *Substitution* (recognizable tone)

- **Other Control Levels:** Passive engineered, active engineered, and procedural (with application of IS guidewords)
  - e.g. *Simplification* of emergency procedures

- **Other design lifecycle stages:** Goal is to evaluate relevant hazards and safety measures before procedure design stage
CONCLUDING REMARKS

- Presented a concept and some thoughts on a design assistance method
- Key objective is to systematically consider the application of all inherent safety principles to all risk control strategies and all process design lifecycle stages
- Essence of our argument – inherent safety is not just a stand-alone strategy that applies only at early design stages
- Considerable further work needed to develop methodology (mathematical rigor and ease of use)
ACKNOWLEDGEMENTS

- Natural Sciences and Engineering Research Council (NSERC) of Canada
- Atlantic Innovation Funded IIC Facility
- Memorial University
- Dalhousie University
- Ministry of University and Research of Italy
- Alma Mater Studiorum – University of Bologna