Application of Bayesian Networks for safety-critical systems in Ammonia plant operations

S. Lee, N. Khakzad, P. Schmitz, G. Reniers, N. Paltrinieri

(to be submitted to Safety Science)

Shenae Lee
6th April 2018
Contents in this presentation:

- Introduction
- Approach
- Case study
- Result
- Conclusion and discussion
Main objective

To develop an approach for

- Using Bayesian network for improving accident probability estimation: Conventional QRA captures a static risk picture.
- Utilizing various information collected from accidents, incidents, inspections etc.
Ammonia plants

- Dangerous chemicals acc. Seveso directive (EU): Ammonia, Hydrogen, Liquefied petroleum gas (LPG), etc.

- The regulation requires risk assessment, and we want to improve the assessment to enhance accident prevention capability

- In general, major accidents continue to occur in ammonia production plants (e.g. Fire in YARA Norge, Oslo, April 2017)
**Introduction**

Major accident scenarios

- Ammonia: Flammable and toxic (toxic inhalation)
  - > Our interest
- Exposure limit (EU)
  - 36 mg/m$^3$ (Acute exposure), 14 mg/m$^3$ (Long term)
- Flammable gasses: Jet fire, Explosion

Safety and risk challenges

- In general, Ammonia plants are outdated (e.g., Many valves manually operated, and automation of valves for vessels inflow and outflow are under consideration)
- Past Ammonia releases indicate technical safety as major importance (e.g., Vessel pressure can quickly build up in case of pressure relief valve malfunction)
- Relevant data on major accident is sparse. We want to make use of data gathered from different plants.
Introduction – general system description
**Step 1 & Step 2**
Scenario in the Bayesian network (BN)

**Step 3 & Step 3.1**
- Nodes for observations are added
- Weights are given to parameter

**Step 4 & Step 5 & Step 6**
Input data to BN is inserted in the existing nodes
Step 1 Bow-tie construction
**Step 2 Convert of bowtie to BN**

**OR gate in a Fault tree**

<table>
<thead>
<tr>
<th>Event</th>
<th>Pr (X1=1)</th>
<th>Pr (X2=1)</th>
<th>Pr (X3=1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**AND gate in a Fault tree**

<table>
<thead>
<tr>
<th>Event</th>
<th>Pr (X1=1)</th>
<th>Pr (X2=1)</th>
<th>Pr (X3=1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Step 3: Add nodes for updating

- Observation from plant 1
- Observation from plant 2

- X1
- X2
- X3
## Approach

### Step 3.1 Calibration of data from different sources

<table>
<thead>
<tr>
<th>Hyper-parameter</th>
<th>Aggregated</th>
<th>Our plant</th>
<th>Other plants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hyper-parameter</td>
<td>$\alpha, \beta$</td>
<td>$\alpha_0, \beta_0$</td>
<td>$\alpha_i, \beta_i$</td>
</tr>
</tbody>
</table>

| Parameter | $\lambda \sim \text{Gamma}(\alpha, \beta)$ | $\lambda_0 \sim \text{Gamma}(\alpha_0, \beta_0)$ | $\lambda_i \sim \text{Gamma}(\alpha_i, \beta_i)$ |

<table>
<thead>
<tr>
<th>AssWeighting</th>
<th>$\alpha = \sum_{i=0}^{n} w_i \cdot \alpha_i$</th>
<th>$w_0 \cdot \alpha_0$</th>
<th>$w_i \cdot \alpha_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$\beta = \sum_{i=0}^{n} w_i \cdot \beta_i$</td>
<td>$w_0 \cdot \beta_0$</td>
<td>$w_i \cdot \beta_i$</td>
</tr>
</tbody>
</table>

where $\sum_{i=0}^{n} w_i = 1$, $w = \frac{1}{\text{rank}} \sum \frac{1}{\text{rank}}$

(According to the zipf's law)
Step 4, 5, 6 Probability updating

Observation from plant 1
Observation from plant 2

X1
X2
X3

Input data
**Case study**

**Safety barrier**

- LICAHL3045 doesn't indicate a low level in V3304
- LICAHL3046 doesn't indicate a low level in V3304
- Inadequate operator action
- PICAHL3032 doesn't indicate a high pressure in V3305
- Inadequate operator action
- Flow orifice pipe SP114 is worn out and doesn't sufficiently maximise the flow
- PSV3014 has failed

**Current analysis**

- Loss of liquid level in V3304
- Pulling pressure control of V3304
- Inadequate operator action
- Loss of liquid level in V3304 at start up
- V3305 has failed

- Loss of liquid level in V3304
- V3305 has failed
- UGALES doesn't indicate a low level in V338
- UGALES doesn't indicate a low level in V338
- Inadequate operator action
- PSV3014 doesn't indicate a high pressure in V338
- Inadequate operator action
- Block-off pipe SP114 is worn out and doesn't sufficiently maintain the flow
- PSV314 has failed
Case study: Pressure Relief Valve (PRV)

Pressure relief valve

Expansion vessel
Case study

Fault tree

Initiating events (Technical)
Initiating events (Operational)
Alarm + Response
Last defense

IE #1
START UP FAILURE TO CONTROL LCV
IE #3
START UP FAILURE TO CONTROL LCV
IE #2
OPERATION FAILURE TO CONTROL LCV
IE #4
OPERATION FAILURE TO CONTROL LCV

Overpressure
TOP

Approach
Result
Discussion
Case study

Event tree

- Rupture (Catastrophic)
- Release stopped, Usgr?&
- Ignition prevented, Usgr?&
- Escalation prevented, Usgr?&
- Suppression succeeded, Usgr?&
- Toxic gas controlled, Usgr?&
- Evacuation succeeded, Usgr?&

Scenarios:
- Safe (Liquid)
- Pool Not ignited
- Pool fire contain
- Pool fire controlled
- Pool fire + No inhalation
- Pool fire + Inhalation
- Pool fire + Fatalities
- Safe (Vapour)
- Cloud Not ignited
- VC/flashfire contained
- VC/flashfire controlled
- VC/flashfire + No inhalation
- VC/flashfire + Inhalation
- VC/flashfire + Fatalities
Bayesian network example (Partial, Liquid control valve)

- **X1**: Level Alarm
- **X2**: OR operator
- **X3**: Automatic control
- **X4**: LCV fail to control
- **X6**: Normal
- **X8**: LCV failure
- **X11**: Normal
- **X12**: Normal

**Introduction**

**Approach**

**Case study**

**Result**

**Discussion**
## Bayesian network example (Partial)

### Basic (root) events

<table>
<thead>
<tr>
<th>Name</th>
<th>Name</th>
<th>Basic event (root) node</th>
</tr>
</thead>
<tbody>
<tr>
<td>X1</td>
<td>OP1</td>
<td>Operator response</td>
</tr>
<tr>
<td>X2</td>
<td>AL</td>
<td>Low Alarm (Level)</td>
</tr>
<tr>
<td>X3</td>
<td>AH</td>
<td>High Alarm (Pressure)</td>
</tr>
<tr>
<td>X4</td>
<td>CL</td>
<td>Controller LCV</td>
</tr>
<tr>
<td>X6</td>
<td>LT</td>
<td>Level Transmitter</td>
</tr>
<tr>
<td>X8</td>
<td>FTC</td>
<td>LCV failure to close (on demand)</td>
</tr>
<tr>
<td>X11</td>
<td>PSV</td>
<td>PSV failure on demand</td>
</tr>
<tr>
<td>X12</td>
<td>FO</td>
<td>Flow orifice (Mechanical) failure</td>
</tr>
</tbody>
</table>

### Intermediate events associated with liquid control during normal operation

<table>
<thead>
<tr>
<th>Dependent nodes</th>
<th>Intermediate (root) node</th>
</tr>
</thead>
<tbody>
<tr>
<td>X1, X2, X3</td>
<td>Level Alarm OR operator</td>
</tr>
<tr>
<td>X11, X12</td>
<td>PSV FO unit</td>
</tr>
<tr>
<td>X1, X2, X3, X4</td>
<td>Level control fail</td>
</tr>
<tr>
<td>X1, X2, X3, X6</td>
<td>LCV not activated_Normal</td>
</tr>
<tr>
<td>X1, X2, X3, X4, X6</td>
<td>LCV fail to control_Normal</td>
</tr>
<tr>
<td>X1, X2, X3, X4, X6, X8</td>
<td>LCV failure_Normal</td>
</tr>
<tr>
<td>X1, X2, X3, X4, X6, X8, X11, X12</td>
<td>Liquid failure_Normal</td>
</tr>
</tbody>
</table>
Updating node probability of pressure relief valve (PRV)

Assumptions

- PRV is the last defense, and the aim is to estimate its realistic failure probability
- From the registration report, the demand of PRV opening is ca. 1 time per year
- Maintenance interval 4 years, time for repair and testing is negligible
- Exponential distribution for dangerous undetected (DU) failure, with perfect repair
**Result**

**Updating probabilities : PRV**

- Use Gamma – exponential conjugate pair

Probability of failure \( \lambda \sim \text{Gamma}(\alpha, \beta) \)
Observation : Failure time \( T \sim \text{Exp}(\lambda) \)

- Update based on (censored) failure times
- Weight is assigned to each \( \lambda \) from Zipf law

<table>
<thead>
<tr>
<th>Source</th>
<th>Rank</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our plant</td>
<td>1</td>
<td>0.545455</td>
</tr>
<tr>
<td>OREDA</td>
<td>2</td>
<td>0.272727</td>
</tr>
<tr>
<td>Other plant</td>
<td>3</td>
<td>0.181818</td>
</tr>
</tbody>
</table>

![Update probabilities diagram](image-url)
Updating probabilities: Operator failures

- Use Beta – Binominal conjugate pair

Probablility of failure $p \sim \text{Beta} (\alpha, \beta)$
Observation: Number of failure $x \sim \text{B} (n, p)$

- Update based on counting number of failures

Where, $n = \text{total number of demand situation (incidence + accident)}$
$x = \text{Operator failures}$
Data source: Public accident data to use generic value
### Reviewed record data for updating

1. For the PRV node: inspection data from our plant

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Substance</th>
<th>Incident type</th>
<th>Origin</th>
<th>General cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>19/6/1998</td>
<td>Columbus, GA</td>
<td>Ammonia</td>
<td>RELEASE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13/10/2007</td>
<td>Repair and major overhaul after valve reassessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Severe damage to the valve most likely caused by frequent (flapping) safety.

2. For the other nodes: related incidence records from the other plants worldwide (since 1983)

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Substance</th>
<th>Incident type</th>
<th>Origin</th>
<th>General cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>29.05.1990</td>
<td>Columbus, GA</td>
<td>Ammonia</td>
<td>RELEASE</td>
<td>PROCESS - PVESS EL</td>
<td>MECHANICAL</td>
</tr>
<tr>
<td>19.02.1991</td>
<td>Geismar, LA</td>
<td>Ammonia</td>
<td>RELEASE</td>
<td>PROCESS - PVESS EL</td>
<td>MECHANICAL</td>
</tr>
<tr>
<td>19.06.1992</td>
<td>Geismar, LA</td>
<td>Ammonia</td>
<td>RELEASE</td>
<td>GENERAL</td>
<td></td>
</tr>
<tr>
<td>28.06.2005</td>
<td>Coffeyville, KS</td>
<td>Ammonia</td>
<td>RELEASE</td>
<td>GENERAL</td>
<td></td>
</tr>
<tr>
<td>11.04.2010</td>
<td>Vatva GIDC</td>
<td>Ammonia</td>
<td>EXPLODE</td>
<td>PROCESS - PVESS EL</td>
<td>PROCOND; INSTRUMENT</td>
</tr>
<tr>
<td>05.11.2015</td>
<td>St.James, LA</td>
<td>Ammonia</td>
<td>RELEASE</td>
<td>GENERAL</td>
<td></td>
</tr>
</tbody>
</table>

3. OREDA (since 1981) and Data from other plants for the baseline (since 1965)
Result

Probability of Ammonia inhalation by operators (on demand situation)

- Toxic cloud, no inhalation: $3.3962 \times 10^{-5}$
- Limited toxic cloud, no inhalation: $0.0033962$
- Toxic cloud AND missile, no inhalation: $3.7736 \times 10^{-6}$
- Limited toxic cloud AND missile, no inhalation: $3.7736 \times 10^{-4}$
- Toxic cloud, inhalation: $3.3962 \times 10^{-5}$
- Limited toxic cloud, inhalation: $0.0033962$
- Toxic cloud AND missile, inhalation: $3.7736 \times 10^{-6}$
- Limited toxic cloud AND missile, inhalation: $3.7736 \times 10^{-4}$
- Safe: $0.99238$

Baseline 1: OREDA
Baseline 2: OREDA + Other plants worldwide
Updated: OREDA + Other plant worldwide + Our plant

Year 1983 Start operation
• **Advantages**
  1) Update our belief about accident frequency after the design phase
  2) Aggregate different data sources with given weights: more specific to our plant
  3) Dependencies between failures (e.g. operator failure and component failures)

• **Limitations**
  1) No consideration of valve degradation
  2) Challenges: collection of relevant data (e.g. PRV registration)