The Relationship Between Automation Complexity and Operator Error

presented by

Russell Ogle, Ph.D., P.E., CSP

Exponent® Failure Analysis Associates

rogle@exponent.com

(630) 274-3215
Control physical and chemical processes to maintain desired conditions

Control agents
- Plant operator
- Basic process control system

Greater automation does not necessarily reduce opportunity for operator error
Reliance on Operators

- Operator often relied on as primary line of defense
- Operator intervention not always successful
- Accident investigation must distinguish between:
  - Operator error
  - System deficiency
Chemical Process Accident

Normal operation

Abnormal conditions

Disturbance grows

Containment strength exceeded

Hazardous release

Disturbance

Operator intervention

Protective systems

Process equipment and control systems

Procedures, training and supervision

Safety instrumented systems and engineering controls

Operator intervention

Procedures, training and supervision

Safety instrumented systems and engineering controls
Human Error Taxonomy

Case Study Analysis

- Layer of protection analysis
- Automation complexity
- Origin of operator error
Layer of Protection Analysis

Independent Protection Layers (IPL):

1. Basic process design
2. Basic process control system
3. Critical alarms and operator intervention
4. Safety instrumented systems
5. Physical protection devices
6. Post-release physical protection
7. Plant emergency response
8. Community emergency response

1 & 2 are not counted as IPL’s

Accident Investigation Focuses on 3, 4 & 5

1 & 2 are not counted as IPL’s

Accident Investigation Focuses on 3, 4 & 5
Automation Complexity

- **Low Complexity**
  - Operator is interacting with single control loop
  - Prone to single event failures

- **High Complexity**
  - Operator is interacting with multiple control loops
  - Prone to multiple event failures
Opération Erreur

- Opération erreur définie comme "déviation d’un désiré en sortie" (Reason, 1990)

- Défi à l’opérateur:
  - Identifier
  - Diagnostiquer
  - Corriger l’altération

- Études de cas suggèrent que la nature de l’erreur est une fonction de la complexité
Case Study Background

- Six case studies involving operator error
- High and low levels of automation complexity
- Impact
  - Six Fatalities
  - Thirty Injuries
  - >$300,000,000 property damage
Table 1. Summary of case studies.

<table>
<thead>
<tr>
<th>CASE STUDY</th>
<th>AUTOMATION COMPLEXITY</th>
<th>AUTOMATION TECHNOLOGY</th>
<th>SAFETY INSTRUMENTED SYSTEM</th>
<th>OPERATOR ERROR</th>
<th>OPERATOR RESPONSE TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 1</td>
<td>Low</td>
<td>Local analog controller</td>
<td>No</td>
<td>Incorrect setpoint</td>
<td>1-2 minutes</td>
</tr>
<tr>
<td>Case 2</td>
<td>Low</td>
<td>Manual operation and SCADA/PLC</td>
<td>No</td>
<td>Wrong order of reactant addition</td>
<td>1-2 minutes</td>
</tr>
<tr>
<td>Case 3</td>
<td>Low</td>
<td>Manual operation</td>
<td>No</td>
<td>Limiting reactant omitted</td>
<td>1-2 minutes</td>
</tr>
<tr>
<td>Case 4</td>
<td>High</td>
<td>DCS and SCADA/PLC</td>
<td>Inadequate</td>
<td>Failure to detect abnormal condition</td>
<td>6 hours</td>
</tr>
<tr>
<td>Case 5</td>
<td>High</td>
<td>SCADA/PLC</td>
<td>Defeated</td>
<td>Failure to detect abnormal condition</td>
<td>4 hours</td>
</tr>
<tr>
<td>Case 6</td>
<td>High</td>
<td>DCS and SCADA/PLC</td>
<td>Defeated</td>
<td>Wrong control action</td>
<td>30 minutes</td>
</tr>
</tbody>
</table>
Case Study 1 Batch Process Oven - Low Automation Complexity

- Parts curing operation
- Evaporate naphtha solvent
- Temperature control via circular recorder controller
- Temperature program via plastic cam
- Temperature ramp
- Positive ventilation

- Operator Deviation ➔ Explosion
Wrong Temperature Cam
Incorrectly Pre-Heated Oven

Pre-Heat

$\Delta T$ from Normal
Case Study 3 Hydrogenation Rxn - Low Automation Complexity

- Liquid + Catalyst + H₂ + Heat
- Add H₂ based on pressure
- Forgot to add unsaturated organic feed
- Manual push-button control, no interlocks
- Heated vessel, but H₂ not absorbed
- H₂ vented through relief system

- Overhead vapor cloud explosion
Pressure Trend – Normal Operation

- Time
- Pressure

- Reaction with Hydrogen Addition
- Blowdown
Pressure Trend – Deviation from Normal

Rupture disc vents reactor
No Reaction
Case Study 4 Polymerization Rxn High Automation Complexity

- Alternating batch reactors for VCM
- Intermediate wash/rinse cycles
- Installation of new Degas Tank
- Process interruption leads to condensed VCM in reactor
- Condensed VCM dumped to atmospheric vessel

- Atmospheric vessel rupture, vapor cloud explosion
Condensed VCM Trapped

- Reactor 1
- Reactor 2
- Degas Tank
- Rinse
- Liquid VCM
- Discharge Tank B
- Seal Pot
- PVC Slurry
- Slurry Tank
Ruptured Storage Tank
Case Study 6 Mineral Processing - High Automation Complexity

- Flash tank section of extraction process
- Electrical power outage
- Operator chose an uncontrolled blow-down
- Low MAWP vessels’ P transmitter ranges exceeded

- High rate of flashing flow; Low MAWP vessels and high P piping explode
Process Controllers

- Automatic Control Set Point
- Actual Value for Control Point
- Controller Output When in Manual
- Dial to Operate Controller When in Manual
- Switch to Right is Manual Control, To Left is Automatic Control
Explosion Damage
Layer of Protection Analysis

- Process Hazard Analysis
  - Hazard
  - Safeguard (layer of protection)

- Allocation of Safeguard Function
  - Operator Intervention
  - Safety Instrumented System
  - Active Safety Device
  - Passive Safety Device
Operator Intervention

- Routine Operations
- Process Upsets
- Startup
- Shutdown
- Emergency Operations
- Emergency Shutdown

What are the operating limits?
  - Consequences of a deviation?
  - Steps required to correct or avoid a deviation?
“Any significant deviation from a previously established, required or expected standard of human performance.”

What Causes Operator Error?

Less than adequate...

- Procedures
- Training
- Supervision
- Communications
- Human Engineering
- Work Direction
- Management System
Conclusions

- Question the effectiveness of operator intervention
- Consider SIS for high hazard emergency shutdowns
- Low automation complexity processes are prone to single event failures – fast to develop
- High automation complexity processes are prone to multiple event failures – slow to develop