INCIDENTS THAT DEFINE SAFE AUTOMATION

• Angela E. Summers, President
• Eloise Roche, Senior SCAI Consultant
• Hui Jin, Risk Analyst
• Mike Carter, Senior SCAI Consultant
• 24 years Chemical Industry background, largely in automation and functional safety management

• Specializes in Safety Controls, Alarms, and Interlocks (SCAI)

• Member of ISA-84 committee and multiple working groups

• Subcommittee Member for revision of “Guidelines for Safe Automation of Chemical Processes”

• Certified Functional Safety Expert
INCIDENTS THAT DEFINE SAFE AUTOMATION

- Angela E. Summers, President
- Eloise Roche, Senior SCAI Consultant
- Hui Jin, Risk Analyst
- Mike Carter, Senior SCAI Consultant
History...

Mexico City – November 1984
500+ fatalities
7000+ injuries

Bhopal, India – December 1984
2000+ fatalities
100000+ injuries

Pasadena, Texas – October 1989
23 fatalities
130+ injuries
6 mile debris radius

Channelview, Texas – July 1990
17 fatalities

Center for Chemical Process Safety (CCPS) - 1985
Process Safety Management (PSM) regulation - 1992

71st Annual Instrumentation and Automation Symposium for the Process Industries
...Repeating

Unfortunately, loss events continue.

Common threads continue to renew focus on deficiencies against principles of Safe Automation:

- Unverified assumptions in PHA or safeguard specification
- Lack of maintenance or timely repair
- Improper use of bypasses
- Changes not recognized or not documented
- New or changed automation not tested adequately prior to startup
- Inadequate training of operators or of staff
- Failure to resolve PHA/Functional Safety Audit findings
## Sample of Events

<table>
<thead>
<tr>
<th>Incident Location</th>
<th>Date</th>
<th>Highlighted Safe Automation Principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Longford, Australia</td>
<td>September 1998</td>
<td>Confirming Hazard and Risk Analysis (H&amp;RA) underlying assumptions</td>
</tr>
<tr>
<td>Hemel Hempstead, England</td>
<td>December 2005</td>
<td>Automation maintenance and timely repair</td>
</tr>
<tr>
<td>Petrolia, Pennsylvania</td>
<td>October 2008</td>
<td>Change management</td>
</tr>
<tr>
<td>Institute, West Virginia</td>
<td>August 2008</td>
<td>Verifying/Validating automation changes</td>
</tr>
<tr>
<td>Illiopolis, Illinois</td>
<td>April 2004</td>
<td>Bypass management</td>
</tr>
<tr>
<td>Ontario, California</td>
<td>August 2004</td>
<td>Training on automation</td>
</tr>
<tr>
<td>Pascagoula, Mississippi</td>
<td>October 2002</td>
<td>Overall automation program management</td>
</tr>
</tbody>
</table>
Introduction to Case Studies

• Based on public reports by investigating bodies or other published references

• One slide summary

• Focuses specifically on the few incident aspects associated to one or more principles of Safe Automation
SCAI Instrument Reliability Program
(ISA TR84.00.03)

• SIL verification includes the following Maintenance and Repair assumptions and design selections
  – Component failure rates, which depend on routine planned preventive maintenance (PPM)
  – Periodic proof testing for dangerous failure modes
  – Mean time to restore after diagnosed failure

• Verification/correction of these assumptions over time requires
  – recording of test/diagnosed failure results
  – escalation of abnormal performance
Ineffective Instrument Reliability Program, Hemel Hempstead, England, December 2005

Key SCAI related gaps:

- Analog level had 14 dangerous failures (stuck) in preceding 3.5 months
- Safety implications of frequent analog level dangerous failures not noted or logged
- 3 level alarms did not activate due to same analog level failure
- High level switch interlock failed due to undermanaged instrument technology change performed by maintenance group ~18 months earlier

43 injuries
2000 evacuated
Commercial and residential damage
SCAI Instrument Reliability Program: Parting Thoughts

• Do procedures ensure “bad actors” are identified, escalated to leadership, and addressed promptly?

• Are content of PPM and testing procedures being correctly updated and maintenance retrained for any changes to device make/model/version?
SCAI Change Management (ISA TR84.00.04)

- When a plant is changed, this potentially changes
  - The causes of incidents
  - The effectiveness of existing safeguards

- This applies whether the change is large or small...
Ineffective “temporary” change management
Petrolia, Pennsylvania, October 2008

Key SCAI related gaps:
- Decision to use operator response to alarm as overfill safeguard instead of the high level interlocks that were on the primary power circuit
- Change and limitations of use were not incorporated into PHA, plant PSI documents, or HMI
- Over many years operators used “emergency” circuit routinely on weekends for years, contrary to original intended use

High level alarm used as normal fill level, and horn not working

1 injured
2500 evacuated from 3 nearby towns
SCAI MOC: Parting Thoughts

- Consider different operating modes, practices or cultures when proposing changes to equipment, or protection strategies in a facility.

- Don’t “set a trap” by using less rigorous engineering and documentation practices for “temporary” changes.

- Audit Process Safety Information (PSI) periodically for discrepancies that develop over time between intended design and practices and current reality.
An approved and well documented change proposal must still be successfully specified, designed and implemented to achieve the intended performance.

Verification and Validation are the practices used to catch human errors made in the specification, design and implementation of instrumented safeguards before lives depend on them.
Key SCAI related gaps:
- Inadequate MOC, including incomplete control system checkout, calibration, tuning, and related procedure updates
- Inadequate DCS training, SOP document, startup expertise
- Inadequate PSSR
- Minimum recirculation flow safety interlock left bypassed by DCS programmers
- Minimum residue treater temperature safety interlock bypassed
- Alarm setpoint ineffective (treater pressure already above maximum and climbing)
SCAI Verification and Validation: Parting Thoughts

• Always use timely verification and validation to ensure automation changes were specified, designed and executed without error or any identified errors are promptly corrected.

• Effective verification and validation reviews require competent independent reviewers.

• Build these tasks, and contingency time to correct any detected defects, into your standard project planning and staffing practices.
SCAI Bypasses – Unsecured? Used too often or incorrectly?

- Hazard analysis practices assume the SCAI will be operational nearly all the time.

- Administrative controls (i.e. operating policies and procedures) on bypasses are subject to the same human errors as the normal operating procedures which may have initiated the event.

- Access restrictions (i.e. keys and locks, passwords) *if done correctly can* mitigate that risk.
SCAI Bypass
Illiopolis, Illinois, April 2004

SCAI related gaps:
- Safety Interlock bypassed with air hose, no authorization, no access controls
- Area alarms ignored by team attempting to mitigate release
- 1992 PHA identified scenario; recommendations not adopted
- 1999 PHA re-identified scenario; rationalized using administrative control
- Similar “near miss” incidents had occurred at another facility the prior year and at the Illiopolis facility about 6 months prior; no corrective actions taken

5 fatalities
3 injuries
150 evacuated
SCAI Bypass: Parting Thoughts

• Do you really need the bypass in the first place?

• Don’t leave keys in the lock or the password written down at the workstation.

• What compensating measures are you using to manage risk during the bypass and are these alternate protections being managed effectively?
Keeping Safe Automation Practices Alive

- ENTROPY - applies to all systems

- Very Simplified Take on Boltzmann’s: Every device/system will break down if you ignore it long enough

- "You get what you Inspect, not what you Expect."

- If you don’t AUDIT the SCAI management systems, they will be broken
CLOSE THE GAPS SOON!

• If you don’t address audit findings in a timely fashion, the SCAI management systems will stay broken

• Broken SCAI management systems WILL result in broken safeguards

• Broken SCAI means under-protected people, environment, and facility assets
Summary

The following safe automation management practices are essential to sustained SCAI effectiveness:

– Verify all PHA/SCAI specification assumptions
– Perform scheduled inspections, testing and preventative maintenance and resolve abnormal performance
– Apply access restrictions AND administrative controls to SCAI bypasses
– Robustly document and manage all changes to PHA or SCAI
– Perform timely verification and validation of new or modified SCAI and correct defects before startup
– Train all personnel involved in safety lifecycle and ensure competence

Competent independent auditing and prompt follow-up on defects is necessary to ensure the above safe automation management practices remain effective.


Questions?