Safety Instrumented Systems in Regulator Station Design

SIL Verification of Standard Design

Alan Burt
Presentation Overview

- Safety standards
- Victorian gas transmission network – Melbourne supply
- History of Dandenong City Gate and design issues
- Project concept and objectives
- AS2885 requirements for pipeline pressure control
- Safety targets and standardised components (SIL)
- Achieving both safety and high availability
- Layers of Protection Analysis of alternate designs
- Conclusions
Definitions

- BLP – Brooklyn Lara Pipeline
- City Gate – gas pressure regulating facility feeding a city
- LOPA – Layer Of Protection Analysis
- MAOP – Maximum Allowable Operating Pressure
- PES – Programmable Electronic Systems
- PLC – Programmable Logic Controller
- PSV – Pressure Safety Valve
- RTU – Remote Terminal Unit
- SIF – Safety Instrumented Function
- SIL – Safety Integrity Level
- SSV – Slamshut valve
- TMR PLC – Triple Mode Redundant PLC
Acknowledgement and Disclaimer

- The author wishes to acknowledge the technical information provided by Invensys – Premier Consulting Services in their report “SIL Assignment and Verification Report” prepared for GasNet for the Brooklyn Lara City Gate.

- The concepts provided herein should not be taken to be endorsement of specific products or design implementation for pressure reduction stations. Designers should assess their specific designs to ensure safety critical and functional control meets the owner’s and technical regulators’ requirements.
Safety Standards – AS/NZS 61508

- AS 61508.3-1999  Functional safety of electrical/electronic/programmable electronic safety-related systems—Software requirements
- AS 61508.4-1999  Functional safety of electrical/electronic/programmable electronic safety-related systems—Definition and abbreviations
- AS 61508.5-1999  Functional safety of electrical/electronic/programmable electronic safety-related systems—Examples of methods for the determination of safety integrity levels
- AS 61508.7-2001  Functional safety of electrical/electronic/programmable electronic safety-related systems—Overview of techniques and measures
Safety Standards - AS/NZS 61511, AS 3814

- AS IEC 61511.1  Functional safety - Safety instrumented systems for the process industry sector - Framework, definitions, systems, hardware and software requirements
- AS IEC 61511.2  Functional safety - Safety instrumented systems for the process industry sector - Guidelines for the application of AS IEC 61511-1
- AS IEC 61511.3  Functional safety - Safety instrumented systems for the process industry sector - Guidance for the determination of the required safety integrity levels

- AS 3814-2005  Industrial and Commercial Gas Fired Appliances
Safety Instrumented Systems

- Safety systems have been used for many years in process industries to perform safety instrumented functions. If instrumentation is to be effectively used for safety, it is essential that this instrumentation achieve certain minimum standards and performance levels.

- AS NZS 61508 addresses Safety Instrumented Systems for all types of industrial applications. A Safety Instrumented System includes all components and subsystems necessary to carry out the safety instrumented function from sensor(s) to final element(s). IEC61511 addresses Safety Instrumented Systems applicable to the Process Industries only.

- AS NZS 61511 applies to Safety Instrumented Systems for the Process Industry that is based on electrical / electronic / programmable electronic technology. Where other technologies are used for logic solvers, the basic principles of this standard should be applied. This standard also addresses the Safety Instrumented System’s sensors and final elements regardless of the applied technology.

- IEC61508 and IEC61511 were recognized by the Australian Standards in the year 2000
AS/NZS 2885.1

- AS NZS 2885 does NOT currently call up AS NZS 61508 nor AS NZS 61511. However, specific levels of control for pressure reduction stations are mandated in AS/NZS 2885.1 clauses 7.2.1 and 7.2.3.

- Safety systems are now commonly used in the gas industry for safety functions in compressor stations, LNG facilities and processing plant, as well as certain ‘Type B’ appliances:

- AS/NZS 3814 requires compliance to AS/NZS 61508 and 61511 for “Type B” fuel-fired appliances controlled by programmable electronic systems. This applies to the following appliances:
  - Gas turbine engines (eg Solar Saturns, Centaurs, Taurus, Mars)
  - Standby generators
  - Waterbath heaters

- For gas pipeline operators, assessment of compliance to engineering principles in AS/NZS 3814, as with other aspects of design for the gas pipeline control, is managed under the Pipeline Safety Case.
Large multi-run pressure reduction stations

- Overpressure protection of pipelines at pressure reduction stations using pressure relief valves may not be acceptable due to offsite hazards.

- Functional requirements for large multi-run pressure reduction stations in Victoria are becoming more demanding due to
  - 4-hourly gas market demands, including frequent remote pressure setpoint control, stop/start operation and interaction with gas compressors
  - Increased pipeline operating pressure, leading to higher pressure drops and potential low temperatures due to Joule-Thompson cooling
Multi-run stations

- Major Victorian multi-run stations (planned capacity)
  - Dandenong City Gate (7 runs)
  - Wollert City Gate (4 runs)
  - Brooklyn Corio Pipeline (BCP) City Gate (5 runs)
  - Brooklyn Lara Pipeline (BLP) City Gate (5 runs)
  - Lara SWP City Gate (5 runs)

- Wollert and Brooklyn projects are currently under construction
- Design is complete for Dandenong and Lara projects
Dandenong City Gate

- Commissioned in 1969
- Initially 2 regulator runs, each with active and monitor regulators and station PSVs
- Growth led to current 7 regulator runs
- RTU to monitor and control pressure
- PSVs replaced with electrical relay over-pressure trip of run inlet valves circa 1979 (ie PSHH trips the station)
- PSVs removed due to proximity of flare
- Slamshut controller replaced with separate RTU circa 1985
- Approximately 65% of Melbourne’s daily gas flows through the station (about 80% annually). The station operates continuously.
Design Issues

- Regulators ‘fail-open’ design
- Inlet valves ‘fail-last’ design
- Common mode failure concern
- Undetected regulator failure
- Operator should not have to open/close runs to avoid overpressure
- Additional heater differential pressure losses affect capacity
- Control algorithms different at other sites
- AS2885.1 requires max MAOP tolerance 1%
- Flow imbalance between runs may lead to noise, erosion and filter failure
Design Concept

- Maintain multi-run station concept (ie retain headers)
- Single active regulator, “fail-closed”
- Upstream slamshut valve (SSV), “fail-closed”
- Standardised control algorithm
- Standardised test program (routine run safety verification tests)
- Remote outlet pressure setpoint control
- Provide improved operator interface (HMI) for maintenance
Project Objectives

- Meet safety objectives per AS61511
- Minimise capital expense
- Pressure control per AS2885.1:2007
- High station availability 99.99%
- Retain contract station differential pressure and peak flowrate design basis
- Maintainability using common sub-components
AS2885.1:2007 Clause 7.2.1
Pipeline Pressure Control

- The following requirements shall be implemented in design and operation of the pipeline pressure control.

- **MAOP under steady state conditions**  For pipelines intended to be operated at a set point equal to MAOP, the control system shall control the maximum pressure within a tolerance of 1%.

- Pressure control and a second pressure limiting system are mandatory. The second (pressure limiting) system may be a second pressure control or an overpressure shut-off system or pressure relief.

- **Pressure control system performance**  Pressure control and overpressure protection systems and their components shall have performance characteristics and properties necessary for their reliable and adequate operation during the design life of the pipeline.
AS2885.1:2007 Clause 7.2.3
Pipeline Facility Control

- Most facilities are remote from their point of operation and generally designed for unattended operation. Each facility shall be designed with a local control system to manage the safe operation of the facility.

- The local control system shall.
  
  (a) Continue to operate in the event of a communications failure;
  (b) If electric powered, be provided with an uninterruptible power supply with sufficient capacity to ensure continuous operation through a reasonable power outage;
  (c) Use reliable technology;
  (d) Be designed to fail in a safe manner; and
  (e) Be designed with appropriate security.

- Each facility may also be configured to enable remote monitoring or control of the facility.
SIL Assignment and Verification

- Analyse SIF “overpressure downstream pipeline”
- Determine SIL achieved using current design with the existing RTUs and regulators
- Determine SIL achievable using proposed design with single FC regulator, SSV and TMR PLC
- Identify required maintenance regime
- Select current BLP project as test case
- Use standard GasNet panels
- Use BLP regulator PID design
Control Schematic for Regulator
PID for Regulator Run
Active Regulator
Regulator characteristics

- Fail closed valve
- Electronic and pneumatic positioner (fails to pneumatic on loss of PES)
- Common station backup pneumatic controller (balances load across runs)
- Diagnostic inputs include closed limit switch and position feedback
- Level 1 fault - valve detected faulty (eg sticky) with persistent control position discrepancy. Run inlet valve closes.
- Level 2 fault – high outlet pressure and control valve not fully closed. Run inlet valve closes.
- Level 3 fault – high outlet pressure. Close all run inlet valves.
- Level 4 fault – high high outlet pressure. Inlet valve closes under pneumatic control.
Fault Tree Models – Pressure Control

Electronic Pressure Control

SIF-10

Fisher DVC6000 (4-20mA) Positioner (exida)

FPCY-62154

6.571E-4

Bristol Control Wave (Defined by AS61508)

RTU

4.257E-2

2

GATE-6-12

GATE-6-13

GATE-6-14

GATE-6-15

Impulse Line - Clean Service (exida)

IMPULSE-LINE-(CLEAN)-PTA

1.095E-3

PT-62755A

2.625E-3

Generic Pressure Transmitter (exida)

IMPULSE-LINE-(CLEAN)-PTB

1.095E-3

PT-62755B

2.625E-3

Generic Pressure Transmitter (exida)

IMPULSE-LINE-(CLEAN)-PTC

1.095E-3

PT-62755C

2.625E-3
Fault Tree Model – TMR Based Control

Site Wide Pressure Control (Tricon)

RF-24A

Triconex Tricon

3.520E-7

TRICON

2 3

GATE-32-0

GATE-27-1

GATE-27-2

GATE-27-3

Impulse Line - Clean Service (exida)

2.500E-7

PT-62755A(R)

9.500E-7

PT-62755B(R)

2.500E-7

PT-62755C(R)

9.500E-7

Generic Pressure Transmitter (exida)

9.500E-7

PT-62755B(R)

9.500E-7

PT-62755C(R)

Generic Pressure Transmitter (exida)

Triconex Tricon

Site Wide Pressure Control (Tricon)
Slamshut valve
Slamshut valve characteristics

- Fail closed valve
- Independent pneumatic high high and low low pressure trip will close the valve
- Electronic open (option) and close control:
  - Open is conditional on outlet pressure
  - Close on PSHH or manual command from DCS or HMI
- Auto/Manual control on slamshut panel. Alarm active while in manual.
Fault Tree – Slamshut system

RF-28 - Slam Shut

Slam Shut

RF-28

Fisher 4660 Pressure Switch Pneumatic (OREDA 84)

PSH-62151

5.700E-6

(Pilot Booster) Generic 2/3 Way Valve (Exida)

PYH-62151A

2.095E-6

(Valve Actuator) Generic 2/3 Way Valve (Exida)

PYH-62151B

2.095E-6

GATE-37-0

Trunnion Ball Valve (Exida)

UV-62151

9.800E-7

Bettis CB Series Valve Actuator (Exida)

UZ-62151

1.630E-6
Fault Tree Model – RTU Whole System
Fault Tree Model – TMR Whole System
# Layers Of Protection Analysis

**Project:** Gasnet Brooklyn Control System Rebuild  
**SIF Identification:** SIF-001  
**SIF Description:** Gas High Pressure

<table>
<thead>
<tr>
<th>Layers of Protection</th>
<th>7m</th>
<th>7b</th>
<th>7a</th>
<th>7e</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact Event</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7a</td>
<td>7b</td>
<td>7c</td>
<td>7d</td>
</tr>
<tr>
<td><strong>Initiating Event</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Likelihood</td>
<td>0.0133</td>
<td>0.0876</td>
<td>0.2</td>
<td>0.0876</td>
<td>0.0133</td>
<td>0.0876</td>
<td>0.2</td>
<td>0.0876</td>
<td>0.0133</td>
<td>0.0876</td>
</tr>
<tr>
<td>Safety Category</td>
<td>Minor</td>
<td>Minor</td>
<td>Minor</td>
<td>Minor</td>
<td>Minor</td>
<td>Minor</td>
<td>Minor</td>
<td>Minor</td>
<td>Minor</td>
<td>Minor</td>
</tr>
<tr>
<td>Target Risk</td>
<td>1.3E-02</td>
<td>8.8E-02</td>
<td>2.0E-01</td>
<td>8.8E-02</td>
<td>1.3E-02</td>
<td>8.8E-02</td>
<td>2.0E-01</td>
<td>8.8E-02</td>
<td>1.3E-02</td>
<td>8.8E-02</td>
</tr>
<tr>
<td>IPL Additional</td>
<td>Pressure Relief Capacity Inadequate</td>
<td>Pressure Relief Capacity Inadequate</td>
<td>Pressure Relief Capacity Inadequate</td>
<td>Pressure Relief Capacity Inadequate</td>
<td>Pressure Relief Capacity Inadequate</td>
<td>Pressure Relief Capacity Inadequate</td>
<td>Pressure Relief Capacity Inadequate</td>
<td>Pressure Relief Capacity Inadequate</td>
<td>Pressure Relief Capacity Inadequate</td>
<td>Pressure Relief Capacity Inadequate</td>
</tr>
<tr>
<td>AIL Additional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actual PFD of the SIF</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
</tr>
<tr>
<td>Mitigated Safety Event Likelihood</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
</tr>
</tbody>
</table>

**Summary:**  
- SIF-001  
- SIL: 0  
- EIL: 0  
- AL: 0  
- Target Risk: 1.0E-01  
- Total Mitigated Safety Event Likelihood: 1.0E-01

**Prepared by:**  
- EIL: Allan Gibson  
- AIL: Alan Burt  
- Date: 16-Mar-07  
- Process Engineer: David Little

---

**Conclusion:**  
- SIL: 0  
- EIL: 0  
- AL: 0  
- Target Risk: 1.0E-01  
- Summary: Occupancy assumed to be less than 876 man hours per year. Ignition data from Oreda Fire and Gas Study.
The safety system for these valves is primarily pneumatic, with the ability to be remotely operated from the network control room and as such is subject to the failure rates of these components and the low accuracy of switching compared to the electronic equivalents.

Adding the electronic diagnostics reduces the failure rate for the pneumatic safety system from 3.6E-2 to 1.05E-2 for the RTU based solution improving slightly to 9.3E-003 for a TMR based solution by bypassing some of the pneumatic logic and providing a parallel trip path. These are however again limited by the reliability of the safety system valves which places a floor under the possible shutdown system performance.

The actual experienced failure rate for the slam shut system has been in excess of 8.26E-3 based on ‘proven in use’ data received from GasNet and this has been used in the above event trees.
Control system implementation

- Assuming the reliability of the Bristol RTU is inline with industrial standards a spurious trip can be expected due to a control system failure at approximately 11.5 year intervals. This means that a failure will probably occur during the life of the plant due to this cause.

- Replacing the Bristol RTU with a typical TMR based system will raise this to the 300 to 3000 year range.

- The probability of a failure of a 2oo3 voting system for the pressure transmitters used in control of either system is so low as to be irrelevant, at $10^{-12}$ per year unless a common cause is considered such as a lighting strike or miss-calibration. These causes are still far less likely than an RTU failure which dominates the probability of failure.
Control and Slamshut Valve Reliability

- Single Control Valve:
  - The Single Control Valve control implementation will result in a failure requiring unscheduled maintenance about every 0.7 years for a station with 5 trains, primarily driven by control valve failures.
  - Installing a TMR based control system will raise this to 0.8 years.

- Dual Control Valve
  - The Dual Control Valve control implementation will result in a failure requiring unscheduled maintenance about every 0.41 years for a station with 5 trains, again primarily driven by control valve failures (i.e., about double the rate for single control valve installation).
  - Installing a TMR based control system will raise this to 0.42 years, a barely noticeable change.

- Slam Shut Valve
  - It is estimated that an individual slam shut valve will close spuriously about every 10 years.
Conclusions

- Safety target is met with one regulator per run provided a TMR PLC is used
  - TMR + Reg + SSV = 2*RTU + 2*Reg + SSV

- For multi-run stations, use of the TMR is more economic because of the cost savings of the regulators. For the same station capacity:
  - Dandenong single regulator solution requires 7 regulators and 7 SSVs
  - Dandenong dual regulator solution requires 20 regulators and 10 SSVs

- For dual run (primary and standby runs) a simpler instrumented design is likely to be more economic.

- Diagnostic systems are required to detect failed/faulty regulator

- Records of failure data or SIL rating are required for all components in the safety system
Program Rollout

- Tricon selected for initial city gate sites at Brooklyn and Wollert
- 2*Trident selected for 4 ea Brooklyn heater BMS
- Interface via TUV serial link to Compressor Station Tricons at Brooklyn and Wollert
- Standard function blocks
- Standard field devices
We Deliver Energy

www.pipelinetrust.com.au