LIFECYCLE ACTIVITIES FOR SAFETY INSTRUMENTED SYSTEMS IN AN ALUMINA REFINERY

Daniels G

Principal Engineering, Rio Tinto Alcan Gove, NT, Australia

Abstract

Introduction:

With new requirements for instrumented protective systems in industry, many end-users are unaware of what this means to them and are treading carefully. New standards have brought new acronyms - SIF, SIS, SIL etc. to the table. The general understanding of these acronyms is not well understood and confusion surrounds which options an end user can or should take. Whilst recommendations are on offer from many consultants, their focus is generally on the design phase of the lifecycle. End users need to understand what installing a compliant Safety Instrumented System will mean to them, as compliance with a defined set of operational procedures is required to prove the ongoing integrity of the protection systems.

Objective:

This presentation provides an insight into an alumina refinery's involvement in the design, installation, operation and maintenance activities of compliant Safety Instrumented Systems (SIS) installed during a major plant expansion. Throughout the lifecycle phases, choices made impact on the ongoing operation and maintenance requirements. This paper discusses the issues encountered at each phase in an effort to assist the end-user in gaining a better understanding of the processes involved.

Approach:

Typical alumina refinery Safety Instrumented Functions (SIF's) are presented. A semi-qualitative approach is adopted for the evaluation phase. Key inputs and outputs are presented for the design and verification phases. A compliance strategy, supporting document system and audit trail are defined for the ongoing maintenance of SIF's.

Key Conclusions:

Much consideration needs to be given to 'which' approach a user should take when installing a compliant SIS system. The option chosen will have a large impact on the ongoing maintenance requirements and users need to be more aware of this. The management of a compliant SIS should not be underestimated and adequate resources are required.

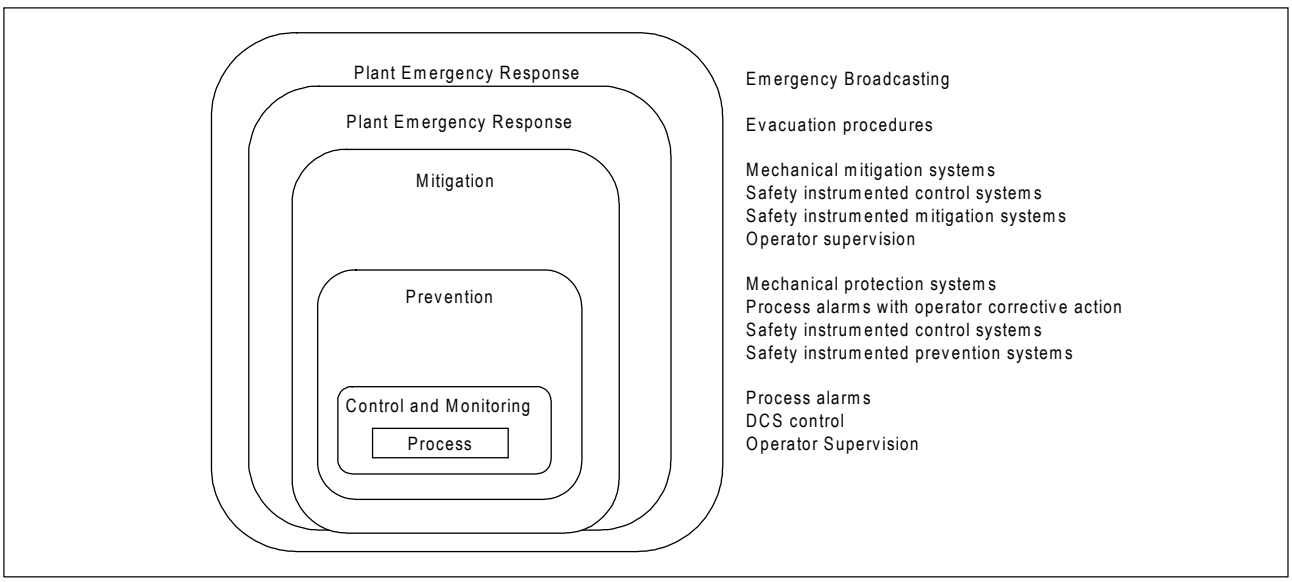
Author:

Greg Daniels CFSE B. App Sc (Dist) AD Elec Eng.

Greg has 25 + years experience in industry, having roles in Electrical Distribution (QEGB), Power Stations (GPS), Mining (BCL), Chemical Plants (ICI) , Smelting (BSL) and Mineral Processing (Nabalco/Rio Tinto Alcan/Rio Tinto Alcan). He has spent the last 11 years with the Gove Refinery. Greg is a Certified Functional Safety Expert (CFSE) with both TUV and with the CFSE Governance Board. He recently represented Rio Tinto Alcan Gove on the G3 project overseeing Control System and Safety Instrumented Systems design and deployment.

1. Introduction

Safety Instrumented Systems (SIS) form part of the layers of protection used to prevent incidents occurring in process plants. The following diagram shows graphically where the SIS typically fits into the overall protection system (AS IEC61511.1 Figure 9).



Typical SIS systems in alumina refineries cover overpressure, overtemperature and Burner Management System (BMS) scenarios. The area/unit based SIS systems and associated Safety Instrumented Functions (SIF's) installed during Rio Tinto Alcan's (RTA) refinery upgrade in Gove Northern Territory, Australia is shown below.

Plant Area/Unit – Logic Solvers	SIF's
Low Temperature Digestion	5 x Overpressure protection functions.
High Temperature Digestion	7 x Overpressure protection functions.
Boiler 1	16 x BMS functions.
Boiler 2	16 x BMS functions.
Boiler 3	16 x BMS functions.
Boiler 6	16 x BMS functions.
Boiler 7	16 x BMS functions.
Calcination 6	25 x BMS functions. 1 x process functions.
Calcination 7	25 x BMS functions. 1 x process functions.
Liquor Purification 1	11 x BMS functions. 5 x process functions.
Liquor Purification 2	11 x BMS functions. 5 x process functions.

This paper presents an alumina refinery's approach to complying with the lifecycle requirements of these SIS systems, as defined in AS IEC61511 - 2004 "Functional safety – Safety instrumented systems for the process industry sector". The content is largely drawn from the RTA - Gove alumina refinery's involvement in the third stage expansion project and subsequent operation of the newly installed Safety Instrumented Systems at that facility. The paper is structured in a format referenced in AS IEC 61511.1 2004 section 4 "Conformance to this International Standard" and shows how clauses 5-19 of that standard have been addressed. Examples are given where possible for illustration.

AS IEC 61511 - 2004 itself is relatively new in Australia and offers many alternatives for implementation. Whilst all of the endorsed approaches have strengths and weakness, the user should be aware what each alternative means for the full SIS lifecycle. Many consultants offer services in the area of SIS design and audit however, the operating and maintenance phases of the lifecycle represent the larger effort and experience here is not widely available.

The purpose of this paper is to present and detail the approach adopted at RTA's alumina refinery in Gove. It is intended as a reference and reality check for other alumina refineries considering AS IEC 61511 compliance. Ultimately the goal is to promote process safety knowledge within our industry and to help keep it safe.

2. Management of Lifecycle Activities AS-IEC61511.1 -2004 Section 5

To complement the existing site Safety Management Policy, a Safety Instrumented Systems (SIS) policy, strategy and audit plan were developed and registered in our factory document management system. It is recommended that the SIS policy/ strategy be a stand-alone document with care not to conflict with existing general safety policies and processes.

Included in these documents is a description of how the lifecycle activities are managed and maintained on site, identifying resources and accountabilities. An example of an accountability structure follows.

Managers	On a plant area basis, ensure • SIS management systems are in place • competent resources are available • proof-testing is completed as per the requirement • approve modification and As Low As Reasonably Practicable (ALARP) recommendations
Engineering	On a site basis, facilitate, manage and document • Safety Instrumented Function identification • Safety Instrumented System design • Safety Requirement Specification (SRS) • Risk Reduction Factor (RRF)/Safety Integrity Level (SIL) determination and verification • Modification and documentation activities • Data collection and improvement processes • Recommendations to area managers in terms of modifications and ALARP. • Verify and audit the installation base. • Report compliance of SIF status to managers quarterly. • Investigate SIS initiated events. • Standards required for proof-testing. • Maintain suitable skills required to manage lifecycle activities.
Operations/ Maintenance	• Perform proof-testing in line with the documented standards, at the required intervals to maintain SIL requirements • Maintain skill level required to perform duties to required standard • Manage, modify and maintain the on-line system. • Manage the installation and start-up phase activities. • Advise Engineering of SIS initiated events • Assist Engineering in development of proof-test procedures.

3. Safety Lifecycle Requirements AS-IEC61511.1 – 2004 Section 6

AS-IEC61511.1 Table 2 was adopted to define the requirements for each SIS lifecycle phase. This is stipulated in the SIS policy/ strategy document.

4. Verification AS-IEC61511.1 – 2004 Section 7

The verification that the outputs of each of the lifecycle phases satisfy the requirements is defined by the processes specified in the SIS policy/strategy document and the audit process.

The SIS design was verified by an independent contractor in the form of a SIL Verification Report or Safety Reliability Report. Further, these reports were cross-checked by our internal experts.

5. Process Hazard and Risk Assessment AS-IEC 61511.1 – 2004 Section 8

Risk Identification

Safety Instrumented Functions (SIF's) were rigorously identified through the design stage HAZOP and CHAZOP processes. HAZOP leaders and minute-takers need to be briefed to seek out and capture potential SIF's and to record them formally. Independent SIF identification reviews were also convened for selected areas. These reviews used plant history, engineering and experience to identify SIF's. SIF review teams were similar in makeup to HAZOP teams, with additional numbers of experienced operators and design engineers.

All identified SIF's were allocated a unique structured ID which is referenced throughout the lifecycle. Identified SIF's are registered in the documentation system whether they were assessed as requiring a SIL rating or not.

An example of an identified Safety Instrumented Function

634SIF3003 "Overpressure of Flash Vessel"

Hazard: Vessel overpressure rupture, extensive equipment damage, loss of containment, boiling.

Cause: Blocked discharge (scale, control failure, human error etc).

SIF Description: Detected by high pressure sensors, trip all slurry and liquor feed pumps.

Assessment methodology

AS IEC61511 offers alternative methods for SIL assessment and in general you can choose between qualitative, semi-qualitative and quantitative approaches. We felt that sufficient data was available across the alumina industry for us to achieve a valid result using a semi-qualitative approach and this also aligned with the site's 'general' risk approach.

In taking this approach it is important to ensure the 'likelihood' scale of the matrix is calibrated against a suitable event frequency. In our case, each of the five likelihood steps were decade based down to 1 / 1,000-10,000 year events. Calibrating the likelihood scale on decades means each 'step' represents a Risk Reduction Factor (RRF) of 10 and a Safety Integrity Level (SIL) of 1. The 'consequence' scale aligned with our previously defined site risk matrix.

The SIL risk matrix, calibration and tolerable levels were also defined in the policy/strategy document and are specific to our safety instrumented functions.

An example: 634SIF3003 "Overpressure of Flash Vessel" Raw Risk (no controls) = Likelihood (Almost Certain) and Consequence (Catastrophic).

6. Allocation of Safety Functions to Protection Layers AS-IEC 61511.1 – 2004 Section 9

The Layer of Protection Analysis (LOPA) method described in AS IEC 61511.3-2004 Annex F was chosen to determine and quantify the amount of risk reduction available in our existing layers of protection. Several LOPA workshops were convened by external facilitators and usually involved 10-15 experienced attendees with strong knowledge of historical industry data/events and a good knowledge of current industry best practice.

Existing layers of protection were identified by the group and each layer was allocated a Risk Reduction Factor (RRF). The RRF is a measure of 'effectiveness' for each of the protection layers and for consistency the SIS policy/strategy document included guidelines on how we allocate RRF. Typical reliability data is available in many SIS related documents however, for the alumina industry special consideration needs to be given for clean or dirty service.

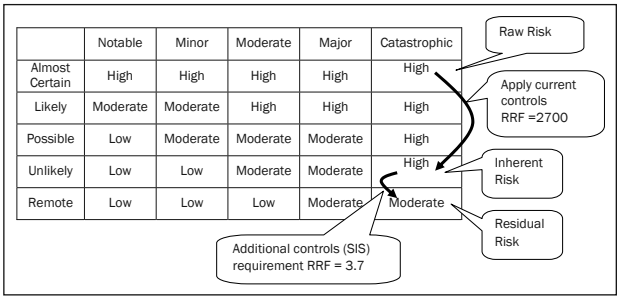
An example of standard RRF allocation guidelines follows.

Layer of Protection	Guideline RRF score
Distributed Control System (DCS) indication/alarm/ control/trip (per individual controller)	3
Maximum RRF in any single controller	9
Independent Hardwired trip, high integrity	10
Pressure relief valves (individual)	10-300
Operator surveillance (trained, effective)	3

An example of typical LOPA allocation for SIF "Overpressure of Flash Vessel" is shown below.

Layer of Protection	RRF
Basic Process Control System (BPCS) Functions (Pressure & Level alarms), (Pressure trip)	9
Relieving devices - 3 x 50% relieving devices, balanced bellows, industry standard devices, pilot operated with steam purge, regular inspection regime.	100
Upstream pressure relief valves restricts maximum pressure	3
TOTAL RRF	**2700**

a) Raw Risk = catastrophic/almost certain
b) Amount of risk reduction required to achieve tolerable level. RRF= 10,000 (4 steps).
c) Present controls provide a RRF = 2700.
d) Additional RRF required = 10,000/2700 = 3.7



e) Team recommends residual risk is reduced to As Low As Reasonably Practicable (ALARP) with a minimum SIS requirement of SIL 1 architecture with a RRF of 3.7.

RRF is the reliability requirement for the design. The impact of SIL 1 definition is further discussed in section 8 of this document

7. SIS Safety Requirement Specification (SRS) AS-IEC 61511.1 – 2004 Section 10

Our policy/strategy document details the general requirements for the SRS and in most cases the specific SRS documents were prepared under contract. Independent SRS documents for each relevant process area or unit (digestion, calcination, Boiler 1 etc) were provided and addressed the requirements for every associated SIF independently. Aligning with our routine shutdown opportunities, our SIS standard Mean Time To Repair (MTTR) for sensors and final elements is set at 12 hours with a proof-test interval of 1 year. Logic solvers have a proof-test interval of 10 years. This meant that after our initial commissioning based 'logic function test' we will only need to test the functional logic every 10 years, however we will need to proof-test the instruments annually.

Sensor voting scheme preferences were specified in order to tolerate a single sensor failure without initiation of a trip timer. Experiences of single sensor failures initiating a trip timer based on MTTR suggest strongly avoiding this configuration.

Another key specification is to ensure all SIS inputs and key logic status points are indicated on the DCS operator screen. It is important to know what is happening in the SIS without the need to analyse logic via the engineering workstation.

The system architecture requirements were specified in terms of Safety Integrity Level (SIL) ratings, and reliability in terms of Risk Reduction Factor (RRF). This is a key to economic design as simply specifying a SIL 1 requirement covers RRF's of 10-99. If we only needed a RRF of say, 16 then specifying SIL1 alone would mean the designers would have to meet a RRF of 99.

In the case of our example we specified a RRF of 3.7 (SIL a) with architecture requirements to SIL1. We also specified a 2 out of 3 voting scheme to allow us to maintain the instruments and auto-rodding devices to ensure clean-service of our sensors.

8. SIS Design and Engineering AS-IEC 61511.1 – 2004 Section 11

The policy/strategy document outlines implementation and equipment specifics for SIS designers. Some key points covered here included:

- Formal design review and approval by client.
- Preferred equipment list.
- Architecture requirements. Single shutoff for SIL1 and below, double shutoffs for SIL2 and above. Sensor voting schemes designed for single failure. No maintenance timers.
- Instrument selection. We used profibus and Foundation Fieldbus instruments for the DCS and conventional instruments for the SIS. Provides independence and diversity.
- SIS motor trip standard circuitry. DCS trips drives via profibus, SIS trips via hardwired shunt circuit. Provides independence and diversity.
- Interface mapping requirements. DCS and SIS interface memory mapping should be defined and designed to minimise data fragmentation.
- Standardization of SIS code between logic solvers.

9. Requirement for application software, including selection criteria for utility software AS-IEC 61511.1 – 2004 Section 12

Application software was written under contract. The contractor submitted their Functional Safety Management Plan which contained documented evidence of their internal quality plan, test regimes and practices. Programmers adopted the use of tested software function blocks and their individual competence was known to us. The project let out the development of the application software based on this.

10. Factory Acceptance Testing AS-IEC 61511.1 – 2004 Section 13

Factory acceptance testing was conducted for all 11 of our logic solver cabinets at the supplier's off-site facility. All FAT's were well structured, documented and witnessed. Testing of every input and output signal using a hardwired panel of knobs, switches, lights and indicators was undertaken. The DCS/SIS interface was also tested using a simulator. The FAT documents are held on site documentation and are auditable.

11. SIS Installation and Commissioning AS-IEC 61511.1 – 2004 Section 14

As defined in the policy/strategy document, a commissioning plan (detailing timing, order of commissioning and responsibilities) and individual SIF test sheets were submitted to the client for approval prior to SIS commissioning. The plan and test sheets included all criteria necessary to fulfil the SRS requirements. Test sheets were specifically related to either the SIF sensors/final elements, other protective devices, logic solvers or procedures and systems.

The test plan included the general order and process requirements to test all of the SIF's. The SIF tests sheets detailed the individual requirements of each test including reference to the relevant proof-test procedures and functional tests. The test plan was approved and the test sheets were witnessed by the client and recorded for validation and audit.

In the case of the example SIF, the test plan may resemble,

a) DCS commissioned as per SAT sheets
b) DCS instruments and logic tested off-line as per test sheets.
c) PRV's setup as per standard, installation checks completed and witnessed.
d) SIS Logic solver commissioned as per SAT document.
e) SIS Individual instruments commissioned as per proof-test instructions.
f) SIS logic function test – no process fluid, simulated inputs. SIS - DCS interface also tested.
g) Operations checks completed.
h) Start-up on-line low flows.
i) Reality checks SIS & DCS instrumentation.
j) Simulate a high pressure to test DCS trip, on-line. Verify actions.
k) Restart at low flow, simulate a high pressure to test SIS trip -line. Verify actions and DCS interface actions.
l) Restart full flow. Simulate high pressure SIS test. Verify actions.

Section 13 Operation and Maintenance - discusses SIS proof-testing and function testing in more detail.

12. SIS Safety Validation AS-IEC 61511.1 – 2004 Section 15

The SIS validation was addressed through the FAT and Site Acceptance processes and throughout the installation and commissioning phases.

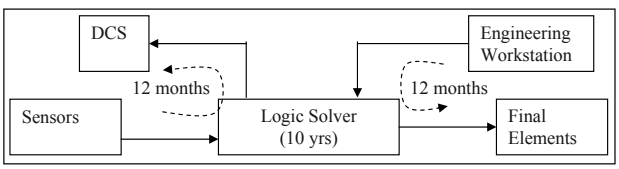
13. SIS Operation and Maintenance AS-IEC 61511.1 – 2004 Section 16

The operating and maintenance phases are required to meet the following objectives,

- To ensure that the required SIL of each safety instrumented function is maintained during operation and maintenance.
- To operate and maintain the SIS so that the designed functional safety is maintained.

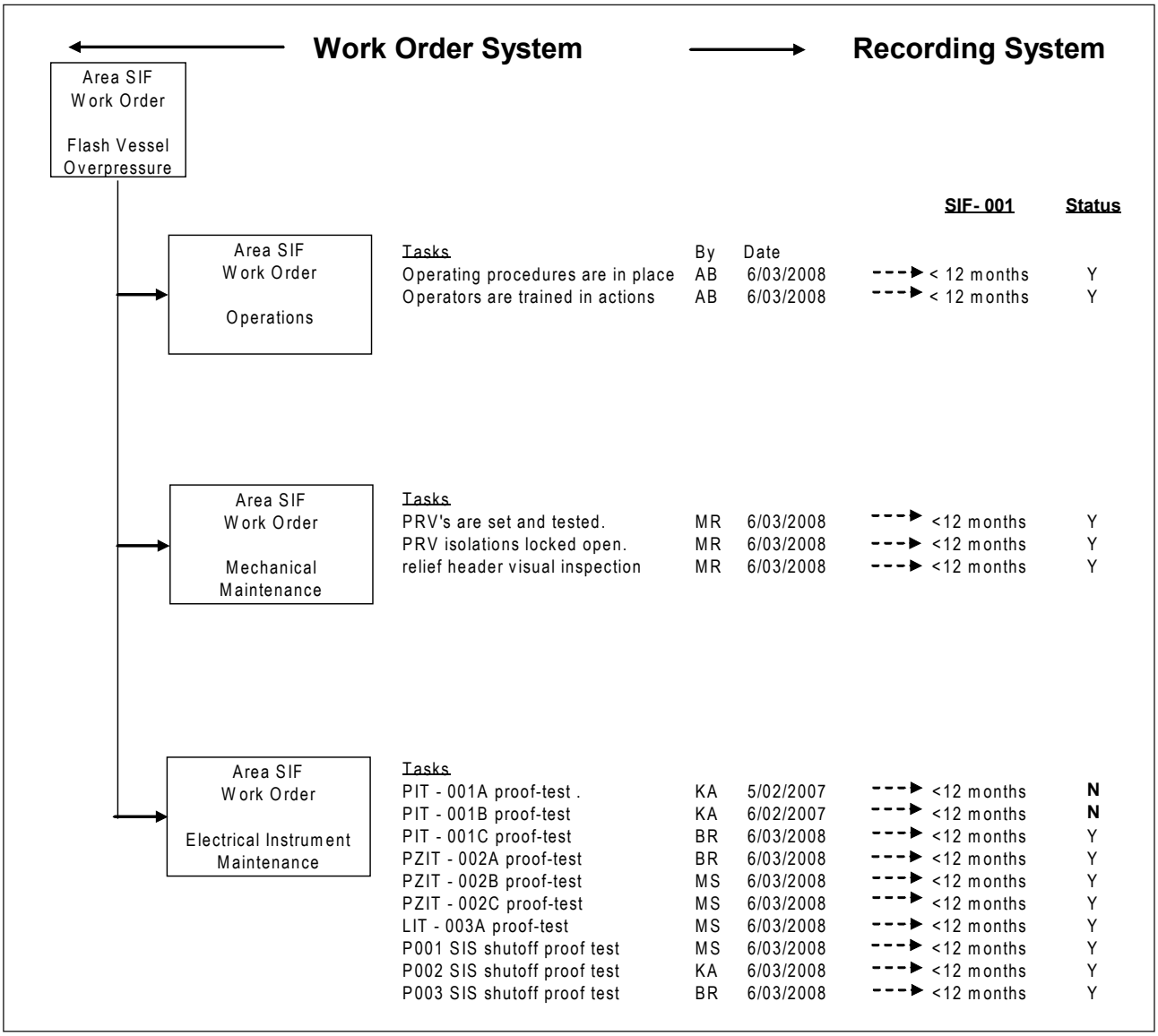
There are two angles needed to address this requirement. Firstly, to achieve compliance, ensure the tasks are completed to the required standard and that this occurs every time. Secondly, determine how to initiate and record the tasks (what vehicle will be used to manage this).

Proof tests are as per detailed task instruction and logic solver tests are as per functional test plans. The following highlights what components are tested.



Proof testing of the sensors and final element require detailed task instructions. Good examples of these can be found through the Health and Safety Executive (HSE) and ISA Technical Reports on SIS proof testing referenced at the end of this paper.

Our site maintenance system (ELLIPSE) provided the tools to generate work-orders and record completion of the tasks, but required two additions to achieve the outcome.



- A recording system that could provide a status of each task on a SIF basis. This would provide a view of the current status of each SIF's test compliance, at any instant.
- The work instruction detail to maintain and proof-test each task. This requires a written task instruction for each activity.

The recording system was developed outside of ELLIPSE and essentially extracts data from the relevant work orders. The task instructions are kept as independent controlled documents and are referenced by the ELLIPSE work orders. The task instruction content is managed under the SIS change control regime.

A flowchart of the maintenance/reporting process is shown below for a typical SIF.

14. SIS Modification AS-IEC 61511.1 – 2004 Section 17

The SIS modification process is documented in the policy/strategy document adheres with the SIS lifecycle approach. The site modification procedure was used as the means to initiate changes however the approval, design, implementation and recording requirements are in alignment with the SIS policy/strategy and can represent considerable effort for even minor changes. The definition of a SIS modification includes changes to any area within the SIS lifecycle including equipment type, proof-testing procedures and documentation.

All of the lifecycle phases outlined in the policy/strategy must be undertaken for each modification.

SIS modifications are registered against the SIF and are recorded in the documentation system.

In general, SIS modifications are rare and are treated cautiously. Due to the low frequency we prefer contractors/assistance to implement SIS modification.

15. SIS Decommissioning AS-IEC 61511.1 – 2004 Section 18

Not applicable to date.

16. Information and Documentation requirements AS-IEC 61511.1 – 2004 Section 19

The document system must be auditable and is recommended to be managed by a dedicated resource. A compliant document system may resemble the sample below.

17. Conclusions and/or Recommendations

Installing a Safety Instrumented System is a cultural step. The decision to take that step indicates an ongoing commitment towards improved process safety and aligns with best practice. The effort required to keep a system compliant should be viewed as an investment in your own people, plant and industry.

Master SIS Document Register

Policy/Strategy		Safety Management Plan Safety Instrumented System Policy Safety Instrumented System Standard
Management of Change - MASTER		Master register- references to area/unit
SIF Area/Unit	Digestion 1	SIL Determination Reports Safety Requirements Specifications SIL Verification/Reliability Reports SIL Validation Reports FAT/SAT Documents Functional Test Plan Proof Test Procedures SIS Instruments - Work Order References Proof-test Work Order System - SIF Status Reports Change Management Audit Procedure Audit Results Support Information
...other area/units..	Digestion "v"	full structure as above
	Calcination 'w'	full structure as above
	Boiler 'x'	full structure as above

Do not underestimate the amount of effort that is required to design, install, manage and maintain a compliant SIS. It is recommended that a dedicated site-based resource is allocated to maintain compliance on larger systems and act as a site contact for SIF lifecycle related issues. For the alumina industry, the semi-qualitative LOPA approach is simple, practical and provides a realistic outcome. This approach is less onerous to maintain than a purely quantitative approach. Defining your requirements in terms of RRF and SIL is more economic than using SIL alone.

Clients must be involved in the early lifecycle phases and need to provide guidelines on contracted activities if they are to manage consistency and maintainability.

Reliability data is important to improving the design and verification phases of any SIS system and is key to improving the SIS process within the alumina industry.

References

AS IEC61511.1 – 2004 Functional Safety – Safety instrumented systems for the process industry sector Part 1: Framework, definitions, systems, hardware and software requirements

AS IEC61511.2 – 2004 Functional Safety – Safety instrumented systems for the process industry sector Part 2: Guidelines for the application of AS IEC61511.1

AS IEC61511.3 – 2004 Functional Safety – Safety instrumented systems for the process industry sector Part 3: Guidance for the determination of the required safety integrity levels

ISA-TR84.00.03-2002 Guidance for Testing of Process Sector Safety Instrumented Functions (SIF) Implemented as or Within Safety Instrumented Systems (SIS) 17 June 2002 The Instrumentation, Systems and Automation Society.

Principles of Proof Testing of Safety instrumented Systems in the Chemical Industry. Contract Research Report 428/2002 prepared by ABB for the Health and Safety Executive.

Area 634 Digestion Safety Integrity Level Determination. Report 2917RPT0001 revision A. PCT Engineers June 2006.