Description of Method for Preliminary Assignment of Safety Integrity Levels (SIL) for the Safety Instrumented System (SIS)

General

The Safety Instrumented System (SIS) consists of sensors, logic solver (ESD) and final elements. The requirement for documentation, management of functional safety and overall safety lifecycle i.e. the activities involved in the implementation of the SIS are described in IEC 61511 and must be adhered to. Likewise compliance with local statutory regulations at the plant location is required.

SIL assessment may according to IEC-61511-3 be done either with qualitative or quantitative methods i.e. using Risk matrices, Risk graphs or Layer Of Protection Analysis (LOPA). The preliminary SIL assessment is done using the attached risk matrices. The final SIL assessment study should be done after the final HAZOP, often in continuation of this. The used risk matrices are to be confirmed.

Qualitative assignment of the SIL is done based on three risk matrices: personal safety, equipment damage / production loss and environmental damage. Refer to Appendices C, D and E. The customer may supply the matrices if corporate standards are to be followed.

The risk matrices are applied without taking the Safety Instrumented System (SIS) into account. However, other protection measures like operating procedures, alarms, safety/relief valves, etc. are taken into account.

The inputs to the risk matrices are the consequences of the incident and the likelihood of occurrence. The required SIL for any given SIF is the highest of the three resulting SIL levels. This is listed on the form in Appendix F.

Appendix C: SIS Personnel Safety Assessment Matrix and SIL Allocation

Safety SIL Assessment Criteria				
Consequence of Incident / **Likelihood of Occurrence**	**Extensive** Several fatalities.	**Serious** Serious injury to one or more persons. Single fatality.	**Minor** Lost time injury requiring hospitalisation.	**Minimal** Minor injury.
High Could happen as often as once a year.	**N/A**	**SIL 3**	**SIL 2**	**SIL 1**
Moderate Could happen as often as once in ten years.	**SIL 3**	**SIL 2**	**SIL 1**	**N/R**
Low Could happen once in lifetime of plant.	**SIL 2**	**SIL 2**	**N/R**	**N/R**

N/A: Not allowed, process redesign required.
N/R: Need not be implemented to a defined level of integrity.

Appendix D: SIS Financial Risk (Equipment and Production Loss) Assessment Matrix and SIL Allocation

Equipment / Production Loss SIL Assessment Criteria				
Consequence of Incident / **Likelihood of Occurrence**	**Extensive** Major equipment damage (>$ 10 million) leading to plant shutdown of more than 7 days.	**Serious** Major equipment damage (<$ 10 million) leading to process downtime of up to 7 days.	**Minor** Equipment damage (less than $ 1 million). Plant downtime of less than 1 day.	**Minimal** Some equipment damage (less than $ 50 000). Negligible downtime.
High Could happen as often as once a year.	**N/A**	**SIL 3**	**SIL 2**	**N/R**
Moderate Could happen as often as once in ten years.	**SIL 3**	**SIL 2**	**SIL 1**	**N/R**
Low Could happen once in lifetime of plant.	**SIL 2**	**SIL 1**	**N/R**	**N/R**

N/A: Not allowed, process redesign required.
N/R: Need not be implemented to a defined level of integrity.

Appendix E: SIS Environmental Risk Assessment Matrix and SIL Allocation

Environmental SIL Assessment Criteria			
Consequence of Incident / **Likelihood of Occurrence**	**Extensive** Serious long-term environmental impact or release.	**Serious** Serious environmental impact outside fence.	**Minor** Complaints of smell or noise, etc. Environmental impact inside fence.
High Could happen as often as once a year.	**N/A**	**SIL 3**	**SIL 1**
Moderate Could happen as often as once in ten years.	**SIL 3**	**SIL 2**	**N/R**
Low Could happen once in lifetime of plant.	**SIL 2**	**SIL 1**	**N/R**

N/A: Not allowed, process redesign required.
N/R: Need not be implemented to a defined level of integrity.

Appendix F: Form for SIL Allocation for Each Safety Function

	TAG NO.	P&I DIAGRAM NO.
INITIATOR(S):		
FINAL ELEMENT(S):		
CAUSE OF UPSET:		
SAFEGUARDS ALREADY IN PLACE:		
CONSEQUENCES:		

Matter of Concern:		Safety	Financial	Environmental
Likelihood:	=			
Consequence:	=			
SIL Level:	=			
Overall SIL Level (Highest Level):				

Documentation and Input Requirements

The functional and safety integrity requirements of the SIS are based on and documented in the following documents:

Piping and Instrumentation Diagrams
Trip diagrams
Operating Manual
Instrument Data Sheets
Instrument Data Sheets for Control Valves
Instrument Data Sheets for Safety Relief Valves
Flare Load Summary
General Specification for the Emergency Shutdown System (ESD)
Description of method for the preliminary assignment of Safety Integrity Level's (SIL) for the Safety Instrumented System (SIS)

Safety Functional Requirements

The trip diagrams show the identified hazards and the shutdown strategy required to bring the plant to a safe state as well as manual shutdown and reset functions. To be confirmed after the final plant HAZOP.

The trip value of each initiator will be given in the Operating Manual together with the alarm and normal operating point. Instrument ranges are found in the Instrument Data Sheets.

Likewise special valve requirements ie. failure action, stroking speed etc. are found in the Instrument Data Sheets for Control valves.

Contingency considered for the safety relief valves are found in the Flare Load Summary.

Functional requirements for the Emergency Shutdown System are given in the General Specification for the Emergency Shutdown System.

Safety Integrity Requirements

Based on the Trip Diagrams each trip group (Safety Function Group) is broken down into safety functions. They are listed at the end of this specification. Each safety function has been given a SIL based on a qualitative analysis using risk matrices; the procedure is described in the document Description of method for preliminary assignment of Safety Integrity Level's (SIL) for the Safety Instrumented System (SIS).

The architecture of each safety function shall meet the hardware fault tolerance requirements as well as the system reliability requirements of IEC 61511.

The diagnostic capabilities of sensors and valves are to be utilised by the logic solver if required to meet the specified SIL.

Testing schedules for sensors and final elements are a function of the implementation method selected to attain a particular SIL. Adequate provision shall be designed into the ESD system for testing back to the primary element without shutting down the process. Likewise testing of final elements during operation may be required if SIL requirements cannot be met due to long turnaround periods.

Field instruments and final elements

Vendors of sensors and final elements which form part of the Safety Instrumented System are to provide details of failure rates, diagnostic coverage and safe failure fraction to be used for the final SIL calculation for each safety function of the SIS.

Package vendors

Package vendors are to provide a safety specification including SIL assessment for each package.

Safety Lifecycle

After the final Plant Hazard and Risk analysis the Preliminary SIL assessments are to be reviewed and modified or confirmed. The safety lifecycle is to be followed during detailed engineering, installation and commissioning, validation, operation and maintenance and finally decommissioning.

Safety functions with Preliminary SIL assessment

On the following pages the Safety Functions are defined and a preliminary SIL is assigned for each.

It has been assumed that:

1) Adequate measures are taken to prevent hazards arising due to explosive atmospheres.
2) The DCS is configured in such a way that a failure will not affect all the additional safeguards for a safety function at the same time.
3) Critical trip initiators are configured as 2oo3 with median extraction. Any significant deviation between initiators is alarmed.
4) Individual pump / blower / compressor trips to be specified by the respective vendors.
5) Control valves in series with SIF final elements are forced to their fail safe position by the DCS which automatically switches controllers to manual mode with output 0% even when the valve is equipped with a solenoid valve.
6) Over pressure protection of the plant is taken care of by safety functions based on other technology i.e. capacity safety valves protect each design pressure level.

Examples

	Tag No.	P&I Diagram No.
Initiator(s):	**FSAL-6070** 2oo3	P07
Final Element(s):	USV-2092/2093/2094 (NG double block-and-bleed DB&B) USV-2010/2043/2048 & USV-2045/2049 (O2 DB&B and SU shut-off) USV-2541/2542/2543 (Fuel gas DB&B)	P10 P02/03 U01

CAUSE OF UPSET:
Control valve/ Controller / Transmitter failure (FIC-6070,FIC-2061 & PIC-2073)
Operator error
NG supply failure

SAFEGUARDS ALREADY IN PLACE:
Low NG feed flow alarm FAL-2061
S/C indication FFI-2069
High temperature alarm TAH-2305
High temperature trip TSAH-2305
Operator action
Flue gas temp. alarms TAH-2295 & TAH-2297

CONSEQUENCES:
Overheating of reformer tubes, reduced tube life, possible rupture
Potential overheating of waste heat section coils

Matter of Concern:		**Safety**	**Financial**	**Environmental**
Likelihood:	=	Low		
Consequence:	=	Minimal	Extensive	Minor
SIL Level:	=	N/R	2	N/R

Overall SIL Level (Highest Level): 2

	Tag No.	P&I Diagram No.
Initiator(s):	**LSAH-2474** 2oo3	P21
Final Element(s):	Partial trip of Syngas compressor C 3001. Block in.	P22

CAUSE OF UPSET:
Control valve/ Controller / Transmitter failure (LIC-2474)
Operator error

SAFEGUARDS ALREADY IN PLACE:
High level alarm LAH-2474
Compressor vibration trip
Operator action

CONSEQUENCES:
Liquid carry-over possible damage to Syngas compressor

Matter of Concern:		**Safety**	**Financial**	**Environmental**
Likelihood:	=	Moderate		
Consequence:	=	Minimal	Serious	Minor
SIL Level:	=	N/R	2	N/R

Overall SIL Level (Highest Level): 2

	Tag No.	P&I Diagram No.
Initiator(s):	**LSAL-2442** 1oo1	P20
Final Element(s):	USY-2446, USY-2450 (stop of Process Condensate pumps 2 MP 2002 A&B) LV-2441 (LUSY-2441)	P20 P20

CAUSE OF UPSET:
Control valve/ Controller / Transmitter failure (LIC-2441)
Operator error

SAFEGUARDS ALREADY IN PLACE:
Low level alarm LAL-2441
Operator action

CONSEQUENCES:
Possible pump damage

Matter of Concern:		**Safety**	**Financial**	**Environmental**
Likelihood:	=	Moderate		
Consequence:	=	Minimal	Minor	Minor
SIL Level:	=	N/R	1	N/R

Overall SIL Level (Highest Level): 1

	Tag No.	P&I Diagram No.
Initiator(s):	**PSAL-7120**	U10
Final Element(s):	USY-7121 (Stop of BFW pump P7001 C)	U10

CAUSE OF UPSET:
Inlet filter blocked
Operator error

SAFEGUARDS ALREADY IN PLACE:
Low pressure alarm PAL-7120 (not all failure modes are independent)
Operator action

CONSEQUENCES:
Pump damage

Matter of Concern:		**Safety**	**Financial**	**Environmental**
Likelihood:	=	Moderate		
Consequence:	=	Minimal	Minor	Minor
SIL Level:	=	N/R	1	N/R

Overall SIL Level (Highest Level): 1

	Tag No.	P&I Diagram No.
Initiator(s):	**LALL-5447** 1oo1	P45
Final Element(s):	UY-5454/5458 (Stop of Off stream pumps P5009 A&B)	P45
CAUSE OF UPSET: Operator error		
SAFEGUARDS ALREADY IN PLACE: Low level alarm LAL-5446 Operator action		
CONSEQUENCES: Pump damage		

Matter of Concern:		**Safety**	**Financial**	**Environmental**
Likelihood:	=	Low		
Consequence:	=	Minimal	Minimal	Minor
SIL Level:	=	N/R	N/R	N/R
Overall SIL Level (Highest Level): N/R				

	Tag No.	P&I Diagram No.
Initiator(s):	**LAHH-6083**	P08
Final Element(s):	USV-6081 (USY-6081) USV-6082 (USY-6082)	P08 P08

CAUSE OF UPSET:
Control valve/ Controller / Transmitter failure
Operator error

SAFEGUARDS ALREADY IN PLACE:
High level alarm LAH-6082
Operator action

CONSEQUENCES:
Overflow of process condensate

Matter of Concern:		**Safety**	**Financial**	**Environmental**
Likelihood:	=	Low		
Consequence:	=	Minimal	Minimal	Minor
SIL Level:	=	N/R	N/R	N/R

Overall SIL Level (Highest Level): N/R