PSIG 1313

Safety Integrity Certification for Pipeline Leak Detection System

René Dietsch

Dow Olefinverbund GmbH
Werk Böhlen, PF 1
04561 Böhlen, Germany
Tel. +49 34206 / 8 – 1603
Fax +49 34206 / 8 – 8188

Dr. Martin Liu, Michael Krätsch,
Dr. Aleksej Lisunkin, Klaus Luber
PSI AG
Dircksenstraße 42-44
10178 Berlin, Germany
Tel. +49 30 / 2801-0
Fax + 49 30 / 2801-1011

This paper was prepared for presentation at the PSIG Annual Meeting held in Prague, Czech Republic, 16 April – 19 April 2013.

ABSTRACT

DOW OLEFINVERBUND GmbH operates a network of ten pipelines for the transport of raw materials and products to and from their production plants in Eastern Germany. Raw materials such as naphtha, condensate and liquid gas as well as products such as styrene, ethylene, propylene or butadiene are transported in the network. The pipelines have a total length of more than 1200 km (745 miles). In accordance with the requirements of the Technical Guideline on Pipelines (Technische Regel für Rohrfernleitungen – TRFL), two continuously operating and independent methods for detecting leaks were required for these pipelines.

A Safety Integrity Level (SIL) assessment – the required effectiveness of safety systems based on the probability of tolerable incidents that can occur within a number of processing demands – was provided in the scope of an overall qualitative and quantitative risk assessment service by the German TÜV. The hazardous classification of the transported fluids requires that the Leak Detection System (LDS) meets the Level 1 safety requirements of IEC EN 61508.

In order to meet the needed Safety Integrity Level, a specific methodology and set of activities were developed. For LDS implementation, a work package was installed in the context of a general facility control system rehabilitation project. The LDS was engineered, installed, put into operation and approved with respect to the SIL 1 requirements under the supervision of the German TÜV.

Up until recently, an LDS was not normally considered a component of a Safety Instrumented System (SIS). However further activities in this area have now begun. The development of the methodology and corresponding practical steps, together with the certification of these steps, are the main benefits of our work.

INTRODUCTION

Functional Safety

The operation of pipelines involves inherent risks due to the presence of dangerous material such as gases and liquids. In the event of emergency, companies have an obligation to limit the risk posed by their operations in order to protect life, equipment and environment.

The instrumentation, automation subsystems, communication equipment, SCADA and monitoring applications are integral parts of an overall system which is subject to functional safety management.

Functional safety management includes methods and measures that minimize hazard risk and environmental impact. The functional safety methods and measures are implemented by means of a dedicated Safety Instrumented System (SIS) or an SIS integrated into general automation solutions for process monitoring and supervision.

Safety Instrumented System

Today it is required to employ an SIS since there is a great potential for losses in the chemical and oil & gas industries. The purpose of the SIS is to reduce risk of a hazardous process to an acceptable level.

An SIS may include one or more Safety Instrumented Functions (SIF) which are designed and implemented to address a specific process hazard or hazardous event.

Typically, an SIF consists of three basic levels: a sensor level, a level of logic solvers and a level of final or control equipment.

Field sensors are used to collect the necessary information which identifies when an emergency situation occurs. The measured process parameters (e.g. temperature, pressure, flow, etc.) can immediately indicate if the technological equipment or process is in a non-safe state. A sophisticated analysis of the process state, which includes advanced data processing on higher levels of the SIS, can also be applied.

The purpose of a logic solver is to evaluate the incoming data, to recognize the risk of hazard occurrence and to determine what action is to be taken based on the acquired information. It is typically a controller that reads signals from the sensors, performs data processing by means of implemented algorithms and executes pre-programmed actions to prevent hazards by providing output to the final control equipment.

The final control equipment (e.g. pneumatically or electrically actuated on-off valves, pumps) executes the defined actions to prevent the hazard situation.

Safety Life Cycle

The Safety Life Cycle (SLC) is an approach that addresses all necessary activities in the implementation of safety-related systems to achieve the required functional safety. The SLC can be subdivided into three phases – analysis, design and development, and operation.

The main focus of the analysis phase is to identify and assess the risks related to hazardous events and corresponding technological equipment. The analysis phase ends when the specification for safety requirements is created.

During the second phase, the functionality and performance criteria for the SIS is designed, engineered, installed, commissioned and validated.

Finally, the operation phase covers startup, operation, maintenance, modification and decommissioning of the SIS.

The SLC approach demands the uniform and systematic consideration of safety functions including the entire life cycle of the technological processes and equipment.

Standards

IEC 61508 is the international standard for electrical, electronic and programmable electronic safety related systems. It is widely accepted as the basis for SIS solutions and covers the SIS specification, design, and operation as well as provides the framework and core requirements for sector specific standards.

The IEC 61511 standard addresses SIS particularly for the process industry including oil and gas production, oil refining and chemicals. IEC 61511 defines practices in the engineering of SIS that ensure the safety of an industrial process through a dedicated use of instrumentation and automation solutions.

The standards cover the requirements for all phases of the life cycle for safety related equipment and functions. It considers Hazard and Risk Assessment methods and defines requirements to SIS design and engineering as well as to tests, installation, commissioning, operation, maintenance, modification, decommissioning and documentation.

Safety Integrity Level

The standards determine Safety Integrity Levels to quantify the risk reduction requirements for a given technological process and corresponding process facility. It represents the required level of SIS functionality with the corresponding performance criteria.

The standards define four safety integrity levels (SIL 1 – SIL 4); a higher level represents higher requirements for the SIS with regard to safety performance criteria.

The SIL classification is an important relationship tool for facility engineering and operating companies to their equipment suppliers as well as to authorities and insurance organizations.

Hazard Risk Reduction Principle

For the elaboration of SIS solutions adequate to the SIL classification, the ALARP principle is usually considered.

The term ALARP stands for “as low as reasonably practicable” and means that the residual risk shall be as low as reasonably possible.

The ALARP is the best common practice of judgment of the balance of risk and societal benefit. It is not a quantified representation of possible hazard risks against costs for implementation of Functional Safety measures related to a given process and facility.

Functional Safety Procedure

The implementation of safety functions includes the following steps:

- Identification of possible hazards and specification of corresponding safety functions;
- Assessment of risks corresponding to safety functions and identification of the required Safety Integrity Level;
- Design of safety functions with their performance criteria taking lifecycle management into consideration;
- Verification and validation of the safety function performance with respect to the defined Safety Integrity Level;
- Functional safety conduction based on audits and evidence assessment as well as application of lifecycle management techniques.

Safety functions are subject to certification with respect to one of the recognized Functional Safety standards and are claimed to a particular Safety Integrity Level. The certification must be issued and periodically inspected by the certification agency. The certification must be supported by a well-developed safety infrastructure. Follow-up surveillance of the safety functions during operation and maintenance ensures that safety function performance is maintained during the entire lifecycle.

IEC 61508 defines SIL requirements by means of two broad approaches or categories: hardware safety integrity and systematic safety integrity. A device or system must meet the requirements for both categories to achieve a required SIL.

Hardware Safety Integrity

The SIL requirements for the hardware or component safety integrity are based on an estimation of

- Safe Failure Fraction
- Hardware Fault Tolerance
- Probability of Failure on Demand or
  Probability of Dangerous Failure per Hour

To achieve a given SIL, the device must meet targets for the maximum probability of dangerous failure and a minimum Safe Failure Fraction with respect to a chosen fault tolerance concept. Today all manufacturers of components relevant for safety implementations provide SIL certified components.

Systematic Safety Integrity

The systematic safety integrity assumes that the hardware or component safety integrity is proven.

With respect to the systematic safety integrity, hazards of a supervised process must be identified by means of risk analysis. The risk reduction is estimated with respect to their overall contribution to identified hazards and specified safety functions required to prevent corresponding hazardous events. The tolerable level of these risks is specified as a safety requirement in the form of a target “probability of a dangerous failure” – a general probability of failure on demand or in a given period of time and stated as a discrete SIL.

Various certification schemes are used to establish whether a device or facility meets a particular SIL rating. The requirements of these schemes can be met either by establishing a rigorous development process or by establishing that the device has sufficient operating history to argue that it has been proven in use.

Further, the procedure is applied for oil and gas pipeline leak risk assessment and for implementation of a leak detection safety function.

Risk assessment for LDS

High Level Safety Function

The primary purpose of a Leak Detection System (LDS) is to support pipeline operators in detecting and localizing leaks. The system provides alarms and displays related data in order to assist him in decision-making. An LDS should always be part of an overall risk reduction strategy or leak prevention program. This minimizes the consequences of leaks if they occur during the transportation of dangerous liquids and gases through pipelines.

Since the LDS is a part of pipeline functional safety it is aligned on different levels to other components including sensors, communication equipment, RTUs (Remote Terminal Units) and PLCs (Programmable Logical Controllers), application servers and operator workstations. Leak detection methods operate on metered data and provide integrated data processing with respect to a corresponding mathematical model. Usually an LDS is a complex application that uses dedicated hardware and software resources.

When an LDS is formally considered as a component of SIS, it must comply with IEC 61508 / IEC 61511 standard requirements and a rating for the required SIL must be performed.

The LDS addresses a specific type of hazards may occur while pipeline is in operation. Here, the pipeline operation is subject to the risk assessment.

Risk Graph

Practical identification of a required SIL for a technological facility or process is provided by means of a risk graph. The following aspects are considered:

- The measure or extension of possible damages for people and the environment;
- The duration of hazard impact on people;
- Possibilities to avoid a direct impact of the hazard on people;
- A rough estimation of the probability of hazard occurrence.

The extension of possible damages for people and the environment is divided into four levels:

- H1: Minor injuries of a person and minor harmful influence on the environment;
- H2: Serious and irreversible injuries of one person or several people or death of a person; major harmful but temporary influences on the environment;
- H3: Death of several people and heavy durable major harmful influences on the environment;
- H4: Catastrophic event, death of lots of people.

The duration of hazard impact is considered as

- O1: Seldom to once in a while;
- O2: Frequently or permanently.

Possibilities to avoid a direct impact of the hazard on people are considered with respect to two categories

- A1: Possible under specific conditions;
- A2: Hardly possible.

A rough estimation of the probability of a hazard occurrence is classified as:

- P1: Very low;
- P2: Low;
- P3: Relatively high.

The Risk Graph depicted on Figure 1 provides considered aspects in relation to each other and maps them on the corresponding Safety Integrity Levels. This Risk Graph is defined by IEC 61508 and provides a rather feasible approach for the risk assessment.

Assessment by Authorities

The SIL rating of a given facility and technological process with respect to the listed criteria is usually provided by third-party experts with respect to corresponding technical, technological, and environmental subject field. Depending on the legal regulations, official boards are also involved in the risk management procedure. Here the Risk Graph is a standardized tool to get the rating.

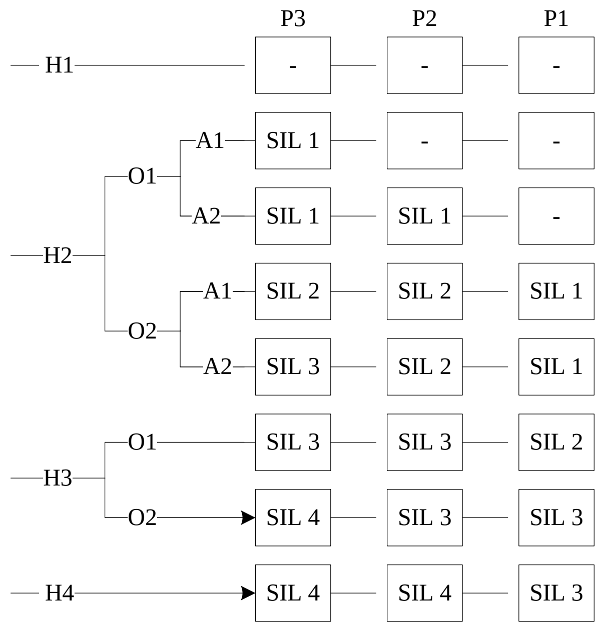

Figure 1: SIL Risk Graph

Risk Evaluation for Transport Pipelines

For oil and gas pipeline systems, the Safety Integrity Level can be considered as follows:

- Damages of pipeline networks could cause serious and irreversible injuries of one person or several people or death of a person. major harmful but temporary influences on the environment may occurs (H2);
- In the vicinity of an accident, several / many people can be located (O2);
- The hazard of the pipeline leak is considered as manageable and direct impact of the hazard can be avoided (A1);
- In general, by operation of the pipeline in proper style, the probability of a hazard situation is considered to be rather low (P1 or P2).

The represented risk analysis leads to SIL 1 rating for pipeline facilities (see Figure 1: SIL Risk Graph).

LDS DESIGN REQUIREMENTS

LDS Performance

The requirements to achieve SIL generally encompass not only the performance characteristics of the LDS but also the LDS development process with verification procedures.

At this time, the LDS evaluation is mainly performed with respect to well-known performance criteria:

- LDS method applicability conditions;
- Typical minimum detectable leak rate;
- Time to leak detection;
- Accuracy of leak localization;
- Occurrence of false alarms.

The estimation of these performance criteria for a given pipeline system and transported media is usually provided in the scope of a dedicated sensitivity study – as one of the beginning phases of such an LDS supply project.

Considering the functional safety life cycle, the sensitivity study is completed at the SIS specification phase, the specified performance criteria are typically inspected during the commissioning, and also verified during the operation by periodically executed tests to check constantly the integrity of the LDS.

LDS Fault Tolerance and Safe Failure Fraction

The issues of the Fault Tolerance and the Safe Failure Fraction are considered in relation to each other. Here, the objective is to define reasonable reliability requirements for leak detection solutions.

The Fault Tolerance defined for safety functions of SIL 1 can be achieved by means of diversity of involved functional approaches and redundant architecture. The Fault Tolerance for LDS is usually considered in accordance with this approach.

The diversity of functional approaches can be achieved when the LDS aggregates several – at least two – independent of each other methods for leak detection, e.g. the mass balance method and the pressure wave analysis. An installation of two completely independent LDS could also be an option.

The redundancy issue is addressed by a supplier of a leak detection solution in the way that he provides fallback mechanisms for his system. Thus, LDS is provided with redundant hardware components, the data processing is performed on redundant components in a hot stand-by or in parallel, i.e. in replication mode. Internal functions and services have to be monitored, any malfunction has to be reported, and any abnormal situation must be supported by a fallback scenario.

In case an LDS supplier does not provide a system with redundant architecture and data processing, a mechanism for continuous monitoring of the leak detection functionality must be facilitated.

An LDS substantially utilizes metered data from field instrumentation. Respectively, the system must possess internal tools and criteria to recognize malfunction of the equipment and to handle abnormal values which may occurs. In case the metered data expresses an excess of information for leak detection, the validation of data must be provided.

SIL 1 does not provide any threshold for the Safe Failure Fraction criterion. Therefore, such threshold is not considered with respect to LDS which has been rated as safety function of SIL 1.

Software Implementation

The software development process must be consistent with the requirements of IEC 61508 life-cycle approach. This approach with the V-Model software development workflow yields a proper organization infrastructure incorporating the safety requirements. In the following, main rules which are crucial for safety related software implementation are summarized:

- Considering safety requirements at a very beginning of the system specification;
- Monitoring and management of functional safety during the system life-cycle;
- Setting up module-based architectures with plug-in techniques for use-case specific features;
- Identification and screening of safety relevant functions and modules;
- Elaboration of application cases with clear specification, development and testing patterns and conventions;
- Extended configurability of software solutions strongly linked with elaborated application patterns;
- Elaboration of extended test case catalogues and testing environment;
- Installing a procedure of test runs over several software releases and use cases;
- Traceability of operation conditions and related software events;
- Management of software and configuration modifications and revisions by means of a release management tools;
- Installing and practicing quality management procedures and tools.

CERTIFICATION AND CONDUCTION

A certification scheme is usually elaborated and validated by the certification board or organization. For the LDS certification, technological approach and technical features of the chosen leak detection solution have to be taken into consideration. The certification scheme addressed below was developed by the German TÜV for leak detection systems based on RTTM with mass balance and pressure gradient analysis procedures:

- Compliance of LDS development with the Functional Safety Management requirements and with a fault reduction business schema (quality management, quality assurance system, documentation, obligatory coding style guide, software verification and validation procedures, test protocols, procedures for software error tracing, revision management and control system);
- Evaluation of Process Flow Diagram (PFD), Hardware Fault Tolerance (HFT) and Safe Failure Fraction (SFF) criteria for basic elements of the LDS (e.g. metering equipment, PLC, etc.);
- Evaluation of software architectures and identification of functional safety relevant components;
- Management and monitoring of safety related functions development and engineering;
- Functional verification of safety relevant components;
- Verification of other software components which interfere with safety relevant components;
- Performing system tests, especially simulating functional errors issued by system components;
- Implementation of performance tests related to functional safety requirements.

The workflow to achieve and adhere to SIL usually consists of two steps: The initial verification and a cyclic verification either periodically or after changes are made.

Initial Verification

The initial LDS verification includes architecture and software code review, as well as audits of development and engineering process. A third-party expert needs to get an overview of the system and business workflow of the vendor. Because the procedure is time-consuming and may involve reasonable human resources, it must be prepared well and extensively supported by the development team of the LDS vendor.

A well-documented and clearly structured business workflow and development process is a necessary condition of the successful evaluation. An unclear structure of the system and imprecise specification of safety functions lead to additional losses of time and resources when system maintenance and modification have to be provided in operation.

The initial verification also includes commissioning and initial operation. Here, system interfaces and data flow are verified. A successful completion of these tests is the necessary condition for the following RTTM and LDS tests.

Further, the metered data are considered in a physically adequate relation to each other by means of the RTTM simulation. For instance, the difference between two metered pressure values must be proportional to the distance between them and hydraulic resistance of the corresponding pipeline section. Here, the simulation provides reference values for the metered data. The occurring deviations must be considered and eliminated. The reason could be metering error, data transmission error, or an imprecise technological description of the pipeline used for the modeling.

After the simulation results are consistent with metered data, functional tests of the LDS can also be performed. The test specification and test execution scenarios must be provided during the system specification and implementation. During the verification phase, respectively to the architecture and principle approach of the solution, partial tests and complex tests are to be proceeded. The test procedures must be accomplished by test records.

If technologically possible, the performance of the LDS is verified by means of real leak tests. In special cases, if the tests may provide a hazard situation for people and the environment, the tests can be performed with simulation or imitation of leaks. In Germany, Site Acceptance Tests of an LDS usually include the leak tests in order to collect evidences to prove the LDS functionality and to assess the achieved performance criteria.

Cyclic Verification

The SIL certification procedure requires from the vendor an appropriate test environment that allows periodical testing of its solution or components in order to check the integrity of the function as close as possible to operation conditions. Routine tests of LDS are usually included by many pipeline operators in the operation schedule, e.g. quarterly or annually.

As an LDS is connected to other equipment, components or subsystems such as field devices, SCADA, instrumentation and communication networks, any change in these subsystems relevant for the LDS performance or integrity must be followed by a partial or complete revision of LDS tests.

Software updates also may change the functionality and performance of the LDS. Hence, software code review also must be considered, although it may take significantly less time as by the initial verification. Here, a proper revision control and management system extracts relevant modifications and minimize efforts. The SIS experts who supervise the LDS must be informed about such modifications. They may also initiate a revision of LDS functional and performance tests.

APPLICATION

DOW OLEFINVERBUND GmbH operates several liquid and gas pipelines with a total length of more than 1,200 km (745 miles) across the eastern part of Germany:

- H_2 in one pipeline;
- Brine in two pipelines;
- Ethylene (supercritical) in one pipeline;
- Ethylene (gas) in two pipelines;
- Condensate and Naphtha in one pipeline;
- Propylene in one pipeline;
- Styrene in one pipeline;
- Butadiene in one pipeline.

In 2011–2012 a facility supervision and control system rehabilitation project was carried out. As part of this project, a special work package has been defined for the rehabilitation of the LDS. The project was engineered, implemented, commissioned and tested under supervision of the German TÜV and in accordance with the SIL requirements.

SIL Assessment

During the evaluation phase, the German TÜV has assessed all quantitative and qualitative risks of the pipeline system operation. As a result, SIL 1 compliant to IEC EN 61508 has been identified and required for LDS. Other components such as instrumentation, automation subsystem and communication network must be certified higher than level SIL 1. The preliminary assessment was documented by TÜV in a technical report (TF-97/601-2).

The corresponding SIL rating for the facility supervision and control system is essential for the permanent operation permission for the pipeline system. In order to meet the required Safety Integrity Level, a methodology including a requirement list as well as specific activities and related procedures have been developed and applied.

Prior to the design and implementation of the leak detection system, a preliminary Functional Safety validation was carried out by the independent experts of TÜV. The main objective of the validation was to analyze:

- The submitted functional specification of the proposed solution including its principle functional features;
- The system architecture and fault tolerance strategy for hardware components and software modules;
- The expected performance of the LDS with the dedicated functional tests procedure;
- Functional Safety Management on site of the solution suppliers and on site of the pipeline operator.

Validation of Requirements

The implemented LDS is based on Real-Time Transient Modeling (RTTM) of fluid pipeline transport and includes Model-Compensated Mass Balance (MCMB) method for leak detection and Pressure Gradient Evaluation procedure for the leak localization.

The LDS must be provided as add-on to the facility SCADA system with a defined communication interface, here – an OPC server-client interface. The following aspects were specified:

- System redundancy architecture with full replication of the function based on two autonomous LDS units connected to two redundant SCADA servers;
- Documentation of input data processing;
- Leak Sensitivity Study;
- Project specific adaptation and engineering of the RTTM;
- Project specific adaptation and engineering of the leak detection and location procedure;
- Tools and features for fault and error handling:

  a) Communication diagnostics;
  b) Threshold violation check for metered data value;
  c) Threshold violation check for metered data gradient;
  d) Comparison of metered and simulated data;
  e) Additional statistical methods for data analysis.

For the software fault tolerance analysis, the LDS vendor has been requested to support the evaluation to provide to the experts and following information:

- Definition of safety related functions;
- Identification of error propagation chains;
- Source code of safety related functions;
- Test scenarios for safety related functionality;
- Certification of critical proven-in-use parts of the software.

For the evaluation of the Functional Safety Management, measures practiced by the LDS vendor are listed below:

- Certification of quality management system in accordance to DIN ISO 9001;
- Establishing of software development conventions;
- Routine validation of a dedicated programming environment;
- Proof and validation of a software revision management system to ensure traceability and transparency of code changes;
- Proof of the competence and experience of the software development team in implementing LDS.

Dedicated Software Validation

Based on the delivered documents, the TÜV experts analyzed the design concept and structure of the system. They reviewed the functional descriptions and test scenarios and checked the safety related functions using an error propagation chain method. This resulted in a catalogue of software test cases including appropriate responses of the software system to different types of input. Upon completion of the analysis phase all safety related functions were reviewed. The LDS vendor had to demonstrate that the software was designed and engineered strictly in accordance to the specification.

LDS Commissioning

The commissioning of the LDS includes verification of the data input, verification of the RTTM and corresponding applications, and preliminary validation of the LDS performance criteria. The commissioning proceeded in close participation of the pipeline operator, the SCADA vendor, and the third-party experts. In particular, the following issues were focused:

- The accuracy of the topological model including geometric and material properties of the pipelines;
- The correct handling of product information (e.g. line fill, density, speed of sound, etc.);
- The correct handling of status information provided by field devices and instrumentation;
- The correct import of metered data and equipment state information from field;
- The accuracy of pressure profiles calculation;
- The accuracy of product temperature profiles calculation;
- The accuracy of product flow calculation;
- The correct handling of product batches;
- The correct monitoring of pig runs;
- The accuracy of mass balance calculation for actively operated and shut-in pipeline sections;
- The calculation of leak locations for simulated data.

During the commissioning phase the LDS vendor had to demonstrate that the system and pipeline RTTM were properly implemented and the data handling yielded correct results.

Final Inspection Assessment

The scope of the final assessment is the verification of the performance criteria of the LDS with respect to specification documents, in particular:

- The system redundancy with respect to fault scenarios;
- The data interface between SCADA and LDS;
- The plausibility of RTTM simulation;
- Processing of safety relevant functions;
- Execution of LDS functions, logging and alarming.

The evidence assessment was performed by execution of real leak tests and leak tests based on the recorded data.

Cyclic Verification

The SCADA system ensures the possibility to superimpose metered values by test sequences for the LDS. In this way, the LDS user is able any time to test almost the complete functional chain of the LDS, beginning with data acquisition, processing and validation, over balance and leak location calculation, to leak logging and alarming.

The LDS test sequences can be recorded during real leak tests or simulated by the RTTM. For this, the LDS vendor also provided an offline simulation tool. The pipeline operator runs monthly tests for the LDS for all pipelines while TÜV participates in the general integrity evaluation of the system once a year.

During the operation, the LDS is maintained by the vendor. The service includes operation support by hydraulic events analysis as well as the software maintenance. In order to guarantee a permanent monitoring of the LDS functionality and integrity, a software review mechanism was established between the LDS vender and the German TÜV. Within this framework, code changes including bug-fixes and software improvements are traced, documented, reported and then approved.

CONCLUSIONS

A Safety Integrity Level assessment was applied to a pipeline network where the leak detection function was considered as an element of Safety Instrumented System. The hazardous classification of the transported fluids provided by the German TÜV requires that the Leak Detection System must meet the level SIL 1. The LDS was engineered, installed, put into operation and approved with respect to the SIL 1 requirements under the supervision of TÜV experts.

The authors believe that this is the first time that LDS for product pipelines of this type have been certified to SIL 1.

ACKNOWLEDGEMENTS

The authors are grateful for the continuous and enthusiastic support from Dow Olefinverbund GmbH, the German TÜV and PSI AG.