Engineering Better Outcomes

Belcan

Technical Note/ September 2021

Design & Functional Safety Solutions for the **Process/Hydrocarbon Industry**

Introduction

Amongst the wide variety of potential hazards associated with operations within the process/hydrocarbon industries, tank overfill scenarios are a well-documented issue and, despite many recent technological and engineering advancements, they are still common occurrences. The stored materials may be hazardous, flammable, explosive, and/or reactive with each other; and a spill may affect drinking water, or if exposed to an ignition source, result in explosions inflicting serious damage to people, property, and the environment. As well as the social and human impacts, the economic impact and associated effects from such incidents can often run into millions or even billions and can pose a threat to a company's survival.

Below we provide a brief overview of a solution provided by Belcan to a major European LNG operator which demonstrates how some of the common challenges with existing plants can be efficiently managed. Additionally, how our systematic approach can be adopted by different process/bulk liquid industries to replicate the achieved results in risk management and compliance to standards/regulations.

Background & Challenges

Overfilling is an identified failure mode of LNG storage tanks, which can lead to loss of containment that, if ignited, may result in fatalities. In this particular scenario, a risk was identified in the site risk register which raised concerns over the current overfill Safety Instrumented Function (SIF) design and compliance with international standards (such as IEC 61511 & 61508) and regulatory requirements. A project was commissioned to ensure compliance and that overall risks from operations were within the acceptable corporate parameters and As Low as Reasonably Practicable (ALARP).

Key project challenges included:

- Over-reliance on operator actions/human response while performing loading/unloading and filling operations
- Inadequate traceability of safety requirements for the SIFs;
- Lack of assurance if risks from overfilling of LNG tanks are ALARP.

Our Solution

Belcan offered a comprehensive multi-phase analysis strategy to identify areas of design improvement and establish auditable and traceable records for demonstrating functional safety compliance with regulatory requirements and international standards.

Concept

- **Site Survey & Design Review**
- **HAZOP Review**
- **Human Reliability Assessment (HRA)**
- **Fault Tree Analysis (FTA) & Safety Integrity Level (SIL) Determination**
- **Design Recommendations**

Detail Design

- **Functional Safety Management & Plannning**
- **BS EN 61511 Desgin Documentation** - SRS, SIL Verification Study, Proof Test Procedures (PTPs), Process Safety Time Estimations, Valve Suitability Analysis, Cost Benefit Analysis (CBA)
- **Process Design** - Updated P&IDs, Control and ESD Naratives & Process Datasheets for Vendor
- **C&I Design** - Updated C&E, Cable Route Diagrams, Cable Schedule, I/O Schedule, Updated JB Schedule, GA & Hook-Up Drawings
- **System Integration** - ESD Functional & Detail Design Specifications, ESD Software Application & DCS HMI, FAT Procedure & Planning
- **FAT Attendance & CAPEX Estimate**

Independent Functional Safety Assessments

- **Stage 1 FSA**
- **Stage 2 FSA**
- **Stage 3 FSA**

Overall Design & System Integration

Key activities as part of system design and integration included:

- Redline mark-ups of Piping &Instrument Diagrams, Reliability and Performance Assessment of Control Valves in Emergency Shutdown (ESD) Application (Suitability Assessment) – including torque analysis, assessment of failure modes, and Weibull distribution analysis;
- ESD Narrative, redline Cause & Effects, deconstruct Cable Route, redline deconstruct Termination Diagram, Updated I/O Schedule, Deconstruct Interlink Wiring; Voltage Drop Calculation, C&I Hook-Up, Solenoid Valve Datasheets;
- Implementation of software application for the ESD System and modification of the process and ESD graphics (HMI);
- Development for the software modification design pack including redline mark-ups of ESD Control Logic extracts (FLDs), Quick Builder Database Mark-Up, ESD I/O Configuration Modifications, Control module modifications in the DCS;
- Factory Acceptance Test (FAT) – Planning and Procedure.

Functional Safety

Belcan delivered the following scope:

- Rationalisation of LNG Tank hazards (HAZOP study review) including Human Reliability Analysis (HRA) to improve the resolution of results and the confidence around assumptions;
- Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) to determine the required integrity for SIFs;
- Sensitivity analysis covering a variety of solutions including key modification parameters for Design, Operations, and Maintenance, SIL verification analysis for all proposed design solutions, and operating regimes to aid design concept selection;
- Cost-Benefit Analysis (CBA) to ascertain the adequacy of potential risk reduction (for the new design) and support ALARP demonstration;
- Update of Safety Requirement Specifications (SRS) and development of proof testing requirements and Proof Test Procedures (PTPs).

Functional Safety Assessment (FSA)

Belcan also commissioned Stage 1 & 2 FSAs for the project by appointing an FS Expert as an independent study chairperson based on the guidelines within IEC 61511 to investigate and verify SIS' achieved functional safety. The FSA aimed to provide confidence that sufficient attention has been given to systematic failures during the design and consisted of:

- A review of organisational compliance (process and procedures) against the requirements of IEC 61511 and documentary evidence of functional safety competence;
- A technical investigation validating that project-specific activities (e.g., risk assessment, engineering, and functional safety assessments) defined under project Functional Safety Management Plan (FSMP) have been carried out with justifiable assumptions, techniques, and adequate coherence exists between all design deliverables.

Belcan Solution

An optimal design modification option was identified and agreed upon for the LNG Tanks, resulting in:

- A new independent layer of protection in the form of "Automatic Closure of Tank Inlet Valves via BPCS/DCS" and reduced vulnerability of the operations to human errors (in respect to overfilling hazards);
- Increased tolerance for SIF's random hardware failures, enabling the client to adopt optimised operations and maintenance regimes;
- Design assurance in respect to FS compliance and ALARP demonstration

  Stage 1 &2 FSA findings and resolution of the resulting actions formed an essential evidence in demonstration of good engineering practice and regulatory compliance expected by the United Kingdom Health & Safety Executive (UK HSE).