Nuclear Engineering and Design 301 (2016) 1–14

Contents lists available at ScienceDirect

Nuclear Engineering and Design

journal homepage: www.elsevier.com/locate/nucengdes

Application of Safety Instrumented System (SIS) approach in older nuclear power plants

Elnara Nasimi, Hossam A. Gabbar*

Faculty of Energy Systems and Nuclear Science, University of Ontario Institute of Technology, 2000 Simcoe St. N., Oshawa, ON, Canada L1H 7K4

HIGHLIGHTS

- Study Safety Instrumented System (SIS) design for older nuclear power plant.
- Apply SIS on Reheater Drains (RD) system.
- Apply IEC 61508/61511 to design safety system.
- Evaluate risk reduction based on proposed SIS design.

ARTICLE INFO

Article history:
Received 11 May 2015
Received in revised form 17 February 2016
Accepted 20 February 2016
Available online 10 March 2016

Classification:
L. Safety and risk analysis

ABSTRACT

In order to remain economically effective and financially profitable, the modern industries have to take their safety culture to a higher level and consider production losses in addition to simple accident prevention techniques. Ideally, compliance with safety requirements start during early design stages, but in some older facilities provisions for Safety Instrumented Systems (SIS) may not have been originally included. In this paper, a case study of a Reheater Drains (RD) system is used to illustrate such an example. Frequent failures of tank level controller lead to transients where the operation of shutting down RD pumps requires operators to manually isolate the quenching water and to close the main steam admission valves. Water in this system is at saturation temperature for the reheater steam side pressure, and any manual operation of the system is highly undesirable due to hazards of working with wet steam at approximately 758 kPa(g) pressure, preheated to 237 °C. Additionally, losses of inventory are highly undesirable as well and challenge other systems in the plant. In this paper, it is suggested that RD system can benefit from installation of an independent SIS system in order to address current challenges. This idea is being explored using IEC 61508 framework for "Functional safety of electrical/electronic/programmable electronic safety-related systems" to provide assurance that the SIS will offer the necessary risk reduction required to achieve required safety for the equipment.

1. Introduction

In today's reality, safety is the primary objective of any utility in power generation, petrochemical or process industry. Normal accident theory suggests that in complex, tightly coupled systems, accidents are inevitable. Thus, every modern plant design will have some built-in protection layers, whether passive or active to provide a defence barrier against known failures. Often, a principle of defence-in-depth is employed, i.e. multiple protection barriers are provided to ensure the risk is minimized. These can be achieved by using either passive or active protection, or a combination of both. A passive protection system does not have any active components, such as actuators or logic solvers and is typically designed using passive components or principles, e.g. gravity drop or concrete containment structure. Active protection

Abbreviations: C/D, capacitance to digital converter; CAD, computer aided design; CANDU, Canadian deuterium-uranium; CCPS, centre for chemical process safety; FEA, finite element analysis; FIT, 1 failure per 109 h; FSN, Fault Semantic Network; FTA, Fault Tree Analysis; HAZOP, Hazard and Operability; HFT, hardware fault tolerance; HP, high pressure; IEC, International Electro-technical Commission; IPL, independent protection layers; LC, level controller; LCV, level control valve; LOPA, layers of protection analysis; LP, low pressure; LT, level transmitter; MPC, model predictive control; NPP, nuclear power plant; P&ID, Piping and Instrumentation diagram; PFD, process flow diagram; PFD, probability of failure on demand; PV, process variable; PWR, pressurized water reactor; RD, Reheater Drains; SD, safe detected; SFF, Safe Failure Fraction; SIF, safety instrumented function; SIL, safety integrity level; SIS, Safety Instrumented Systems; SU, safe undetected.

* Corresponding author. Tel.: +1 905 721 8668x5497; fax: +1 905 721 3046.
E-mail address: hossam.gabbar@uoit.ca (H.A. Gabbar).

http://dx.doi.org/10.1016/j.nucengdes.2016.02.026
0029-5493/

systems can be implemented in a variety of ways, ranging from electro-mechanical relays and solid-state electronics to complex programmable electronic devices. In safety-related applications it is common to incorporate programmable logic controllers, microprocessors, integrated circuits, and other programmable devices such as smart sensors, transmitters and actuators. Safety Instrumented Systems (SISs) have been used in a broad variety of process industries.

Ideally, compliance with the safety requirements starts as early as during design specifications and continues through installation, testing and maintenance of Safety Instrumented Systems. However, in some older facilities, as will be seen later in this paper, the provisions for Safety Instrumented Systems and multiple safety barriers may not be adequate in today's view of how to effectively minimize process risks and lower production losses to a tolerable level. This paper makes an attempt to assess feasibility and benefits of application of Safety Instrumented Systems (SIS) principles, followed by a high-level conceptual proposal for integration of SIS into an existing system at one of the typical older nuclear power plants to address ongoing operational and safety challenges.

1.1. IEC standards for functional safety and process system safety

In order to remain economically effective and financially profitable, the modern industries have to take their safety culture to a higher level and consider production losses in addition to simple accident prevention techniques. Effective safety management has to include reliability program, design and configuration management, instrumentation quality assurance and effective vendor oversight at all levels of the supply chain. Although zero risk can never be achieved, organizations should strive for a high degree of reliability, especially in special safety systems not only to reduce the risks but in order to maximize safe production. Thus, the objective is to ensure that all equipment performs reliably through the operating cycle, and standby safety equipment operates properly on demand.

In 1998 the International Electro-technical Commission published IEC61508 document titled: "Functional safety of electrical/electronic/programmable electronic safety-related systems" (Functionalsafety, in press). This document sets the standards for safety-related system design of hardware and software. Three sector specific standards have been released using the IEC 61508 framework, IEC 61511 (process), IEC 61513 (nuclear) and IEC 62061 (manufacturing/machineries) (IEC, in press). IEC 61511 Standard was developed specifically for industrial processes where safety functions are implemented using modern instrumentation, or so-called Safety Instrumented Systems (Houtermans, in press). IEC 61511 sets out the requirements for ensuring that systems are designed, implemented, operated and maintained to provide the required Safety Integrity Level (SIL) (Medoff and Faller, in press). It provides the assurance that the safety-related systems will offer the necessary risk reduction required to achieve safety for the equipment. It defines four SILs according to the risks where SIL4 is assigned against the highest risk.

1.2. Safety Instrumented Systems

A Safety Instrumented System (SIS) is composed of independent trains of sensors, logic solvers, final elements, and support systems that are designed and managed to achieve a specified safety integrity level (SIL). Based on the sensor data from the field, the SIS logic solver determines whether the process system performs as expected and the process variables (PVs) are within their expected allowable band. Plant data is compared to the system model parameters and actuator is engaged if adjustment is required. The actuator action can be as little as a minor valve adjustment or as critical as a process shutdown. For each specific process hazard or hazardous event an SIS performs safety instrumented functions (SIFs), which are designed to address and maintain the predefined safety goals (O'brien, in press) (Fig. 1).

It is important to point out that Safety Instrumented Systems have no part in process regulation (Punch, in press; Smith and Simpson, in press). Process control loops maintain process variables (PVs) within prescribed upper and lower allowable limits, while the SIS monitors a process and only takes action when required.

2. Literature review

There are many traditional mathematical, statistical and visual methods used to describe design and energy flows for complex industrial systems such as automotive, railway, chemical or power plants (Reedy and Lunzman, 2010; Gani and Pistikopoulos, 2002). In a model-based approach, a complete system is designed and debugged using tools such as MatLab Simulink. System control codes and responses are tested and optimized in order to minimize the required engineering support during commissioning. For example, as described in (Reedy and Lunzman, 2010) a completed drive train control system model was built and tested in simulation environment to refine control strategy prior to field commissioning. Similarly, the use of property models in product/process simulation and design is highlighted in (Gani and Pistikopoulos, 2002). This work shows the role that property models play in simulation and design from a user's point of view, e.g. during simulation of a distillation operation, the property models provide values for fugacity coefficients, enthalpies, etc. when requested. Similar to process industries, MatLab/Simulink tools are commonly used by control designers for nuclear reactors to implement high fidelity real-time control models. These tools are particularly suitable for time and frequency response analysis or system logic stability tests and will be used in this work to represent key aspects of a real-world system in the selected case study.

Traditional modeling approach can be based on actual process data or be first principles-based (Michael, 1993). Modeling based on first principles is based on creating a block diagram model that implements known differential-algebraic equations describing plant dynamics. Well-known application of physical modeling is piping design, described in (Michael, 1993). Piping design consists of planning the number of sections and components required to move the desired material. Next, piping analysis is conducted to analyze load versus time at various locations in the system. Computer-aided design (CAD) and finite element analysis (FEA) software can be applied to the creation of piping systems, as well as to other mechanical systems. This method was considered to be used in the selected case study but was eliminated for a number of reasons. First, each element in this model is selected to represent a portion of the plant. Its connections in the model show relationships between various components and parts. Plants represented by block diagrams are typically very simplified and have to be augmented with process flow diagrams to indicate correct streams of energy or material flow. This is particularly important in this work, as the main emphasis is on the control system modifications and upgrades, rather than on physical properties of tubes, piping or tanks used in the plant. Next, plant model based on PFD or P&ID tools has no fault forecasting or behavior analysis capabilities. This becomes particularly important during design validation and verification stages of this project and may present certain challenges during implementation phase in the field. If it were sufficient to use only piping layout of the process along with the installed equipment and instrumentation, Piping & Instrumentation diagram (P&ID) could be used.