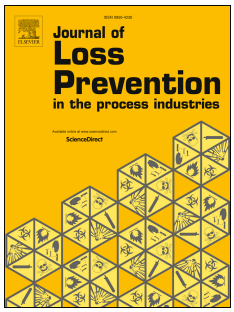
Accepted Manuscript



How and when do I validate, proof test and Re-validate my SIS logic solver?

Prasad Goteti

PII: S0950-4230(18)30007-X

DOI: 10.1016/j.jlp.2018.06.008

Reference: JLPP 3719

To appear in: *Journal of Loss Prevention in the Process Industries*

Received Date: 3 January 2018

Revised Date: 12 June 2018

Accepted Date: 14 June 2018

Please cite this article as: Goteti, P., How and when do I validate, proof test and Re-validate my SIS logic solver?, *Journal of Loss Prevention in the Process Industries* (2018), doi: 10.1016/j.jlp.2018.06.008.

How and When do I Validate, Proof Test and Re-Validate my SIS logic solver ?

Prasad Goteti,
P. Eng, FS Expert (TÜV Rheinland), CFSE
Safety Engineering Consultant
Honeywell Process Solutions
Houston, TX, USA

KEYWORDS

Basic Process Control System (BPCS), Distributed Control System (DCS), Safety Integrity Level (SIL), Safety Instrumented Function (SIF), Safety Instrumented Systems (SIS), Proof Test Interval (PTI), Diagnostic Test Interval (DTI), Validation, Proof Test, Re Validation,

INTRODUCTION

A major component of every Safety Instrumented System (SIS) is the Logic Solver. It plays an important role as it is the sub-system which performs the logic in every Safety Instrumented Function (SIF). But sometimes there is confusion as to what constitutes:

1. Validation of the SIS logic solver
2. Proof Test of the SIS logic solver
3. Re-Validation of the Logic Solver

This paper will attempt to clarify the above with an explanation based on IEC 61508, 61511 (ISA84.00.01). It will answer the questions “When and How” for each of the activities listed.

BASIC CONCEPTS

A Safety Instrumented System (SIS) is a system that implements Safety Instrumented Functions (SIF) to maintain or to bring back a process into a safe state. Those SIFs are classified into four different levels depending on the probability that they will be successful when asked to perform. That probability based level is known as the Safety Integrity Level (SIL).

A SIF is composed of three distinct sub-systems: Sensor elements that detect certain process conditions, a logic solver that through some logic determines if those conditions are unsafe and sends commands to restore a safe state, and actuating devices that act on the appropriate process variables, executing the commands of the logic solver. So for a SIF to meets its SIL value, all three sub-systems need to perform with a certain amount of reliability.