



OTC 18504

## High-Integrity Protection Systems (HIPS): Methods and Tools for Efficient Safety Integrity Levels Analysis and Calculations

Jean-Pierre Signoret, Total

Copyright 2007, Offshore Technology Conference

This paper was prepared for presentation at the 2007 Offshore Technology Conference held in Houston, Texas, U.S.A., 30 April–3 May 2007.

This paper was selected for presentation by an OTC Program Committee following review of information contained in an abstract submitted by the author(s). Contents of the paper, as presented, have not been reviewed by the Offshore Technology Conference and are subject to correction by the author(s). The material, as presented, does not necessarily reflect any position of the Offshore Technology Conference, its officers, or members. Papers presented at OTC are subject to publication review by Sponsor Society Committees of the Offshore Technology Conference. Electronic reproduction, distribution, or storage of any part of this paper for commercial purposes without the written consent of the Offshore Technology Conference is prohibited. Permission to reproduce in print is restricted to an abstract of not more than 300 words; illustrations may not be copied. The abstract must contain conspicuous acknowledgment of where and by whom the paper was presented. Write Librarian, OTC, P.O. Box 833836, Richardson, TX 75083-3836, U.S.A., fax 01-972-952-9435.

### Abstract

This paper shows how to deal properly with "Safety Integrity Levels" (SIL) as per IEC 61508 [1] and 61511 [2] for "High Integrity Protection Systems" (HIPS) which are more and more extensively used in oil industry to replace traditional protection systems. If IEC 61508/511 are rather efficient from an organizational point of view, some difficulties unfortunately exist at definition and calculation levels. The formulae proposed in part 6 of IEC 61508 are, for example, not really tractable for actual industrial systems. This paper describes the probabilistic methods and tools that we have developed in our company to overcome the above difficulties. Three main conventional methods are investigated: "Fault Trees" which, when properly handled, are very efficient for low demand topside HIPS, markovian approach which is interesting but tractable only for very small systems and Monte Carlo simulation on behavioural models (Petri Nets or AltaRica Data Flow formal language) which is efficient in any cases. Results are given on simple examples in order to show the principles of the various approaches. It is interesting to notice that using those approaches is simpler than what is proposed in the standards. Therefore, until the publication of an updated version improving IEC 61508 part 6, it seems better to replace it by sound conventional methods and tools adapted to SIL calculations for production systems. We have begun to disseminate this approaches toward our contractors.

### Introduction

In the oil industry, the traditional protection systems defined in API 14C are more and more often replaced by safety instrumented systems: the so-called HIPS (High Integrity Protection Systems). Therefore, according to IEC 61508 and IEC 61511 Standards, their SILs (Safety Integrity Levels) shall be calculated

Unfortunately, when using above standards some difficulties arises [3, 4]. They often remain ignored by those who perform SIL studies and the main ones are the next:

1. insufficient failure taxonomy and definitions,
2. tests and maintenance procedures handling,
3. introduction of the Safe failure Fraction (SFF) which is not a relevant concept,
4. probability of Failure on Demand (PFD) and Probability of Failure per Hour (PFH) Calculations.

After presenting briefly the 3 first problems, the 4<sup>th</sup> one will be detailed more in depth to show what we have done to cope with the various SIL assessment problems encountered in the oil industry:

1. topside HIPS easily tested and maintained,
2. subsea HIPS difficult to test and maintain,
3. preventive HIPS.

According to the standards topside and subsea HIPS are so-called "*low demand mode*" safety instrumented systems (SIS) while preventive HIPS are so-called "*continuous*" mode SIS. This paper is mainly focused on methods and tools devoted to low demand mode HIPS.

### Failure taxonomy

In IEC 61508 and 61511 standards the failures are split into *dangerous* or *safe* and *detected* or *undetected*. This is a little different of the classical failure taxonomy:

- *safe* versus *unsafe*,
- *revealed* versus *hidden*,
- *time dependant* versus *on demand*.

If the *dangerous* failure definition is very similar to the classical *unsafe* failure (i.e. a failure which tends to inhibit the safety function) this is not the case for the *safe* failure. In the standards it is only a failure which is not dangerous when in the traditional approach this is a failure which tends to anticipate the safety action.

The classification "*detected* versus *undetected*" of the standard is similar to "*revealed* versus *hidden*". The problem is that the users reading the standards too quickly thought that they can assimilates straightforwardly revealed failures with safe failures. Of course this is generally not true.

Among the third class of failures, only the *time dependant* failures are recognized by the standards. The true "*on demand failure*" are completely ignored and, even worse, are hidden behind the term *Probability of Failure on Demand* (PFD) which encompasses only time dependant failures occurred during the test interval. This is a big problem as those failures