Reliability Engineering and System Safety 180 (2018) 111–123

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Modeling patterns for reliability assessment of safety instrumented systems

Huixing Meng*,[a], Leïla Kloul[b], Antoine Rauzy[c]

[a] Laboratory of Computer Science, École Polytechnique, Paris, France
[b] DAVID, Université de Versailles St-Quentin-en-Yvelines, Versailles, France
[c] Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, Trondheim, Norway

ARTICLE INFO

Keywords:
Modeling patterns
Reliability assessment
Safety instrumented systems
ISO/TR 12489

ABSTRACT

Safety Instrumented Systems (SIS) act as crucial safety barriers for preventing hazardous accidents in the industrial systems. It is therefore of primary importance to study their reliability, i.e. eventually to design probabilistic reliability assessment models. SIS have common behaviors such as the periodic test policies to reveal the dangerous undetected failures. These common behaviors can be captured in models via modeling patterns. By reusing modeling patterns, the modeling process can be simplified and made more efficient.

In this paper, we propose a versatile set of modeling patterns implemented in AltaRica 3.0 language. We apply them to assess the reliability of SIS described in ISO technical report ISO/TR 12489. Comparisons are performed between the results obtained from AltaRica models and those reported in ISO/TR 12489. We show that the set of proposed modeling patterns can serve as an effective tool to model SIS in a modular way.

1. Introduction

Safety Instrumented Systems (SIS) act as crucial safety barriers for preventing hazardous accidents in the industrial systems. These systems are composed of sensors, logic solvers, and final elements. Logic solvers translate signals transmitted from sensors into decisions made on final elements. SIS have attracted tremendous attention from various industrial sectors. Associated standards are proposed in several industries, such as the process industry [1], the nuclear power industry [2], the machinery industry [3,4], the automotive industry [5], and the railway industry [6–8]. The main standard is IEC 61508 [9]. The sound performance of SIS is crucial for the industrial systems.

It is therefore of primary importance to study the reliability of SIS, i.e. eventually to design probabilistic reliability assessment models. Reliability studies of SIS have been conducted extensively (see e.g., [10–13]) including proof tests [14–16], k-out-of-n voting structures [17–20], common cause failures [21–24], spurious failures [25,26], human and organizational factors [27,28], uncertainty [29–32], and optimization issues [33,34].

Modeling experience is expected to be capitalized. Otherwise, the modeling activity is unlikely to be profitable. Patterns can be utilized for reusing stabilized knowledge. However, few studies have been conducted on modeling patterns for reliability assessment of SIS.

Patterns were first formally proposed in civil engineering [35]. They have been adopted in software engineering subsequently as design patterns, which are descriptions of communicating objects and classes that are customized to solve a general design problem in a particular context [36]. A design pattern promotes design reuse, conforms to a literary style, and defines a vocabulary for discussing design [37].

A modeling pattern is a general means allowing to capture the frequently recurrent component and subsystem behaviors. Some researchers try to provide a general framework of reusing patterns. The Pattern Based System Engineering (PBSE) was proposed to develop configurable and reusable system models [38]. A PBSE procedure includes the pattern definition and the system development with patterns [39].

The reuse of systems and subsystems is a common practice in safety-critical systems engineering [40]. To reuse system behaviors, we need to standardize the representation of reusable components and clarify the way they exchange information [41]. The whole point of a pattern is thus to reuse, rather than to reinvent [37].

An advantage of high-level modeling languages, like AltaRica [42], is to *reuse* models of components or even systems [42]. The AltaRica modeling language is introduced in IEC 61508 as a technique for calculating probabilities of hardware failures in SIS [9]. The language is also referred in ISO/TR 12489 [10]. AltaRica has become a defacto European industrial standard for model-based safety assessment [43].

In this study, we propose a set of modeling patterns for reliability assessment of SIS. We classify the proposed modeling patterns into three categories. We implement these modeling patterns with the

* Corresponding author.
E-mail addresses: Huixing.Meng@hotmail.com (H. Meng), Leila.Kloul@uvsq.fr (L. Kloul), Antoine.Rauzy@ntnu.no (A. Rauzy).

https://doi.org/10.1016/j.ress.2018.06.026
Received 27 December 2017; Received in revised form 20 June 2018; Accepted 25 June 2018

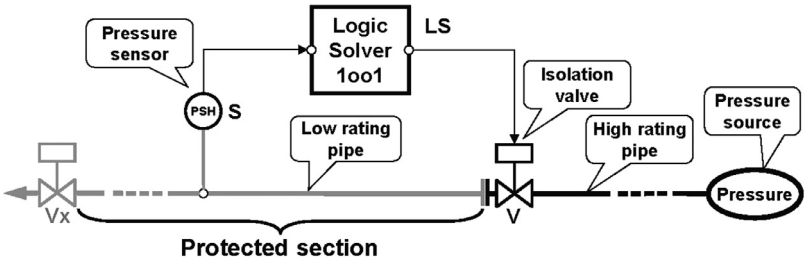

Fig. 1. An overpressure protection system with a single channel [10].

AltaRica 3.0 language. We apply these modeling patterns on all SIS in ISO/TR 12489. Preliminary results of this study have been presented at a symposium [44].

The rest of this paper is organized as follows. Section 2 reviews the related works. Section 3 introduces the SIS described in ISO/TR 12489. Section 4 is dedicated to present the modeling patterns extracted from the above SIS. Section 5 discusses the modeling patterns in the framework of guarded transition systems, i.e. the mathematical background of AltaRica 3.0 language. A methodology of reusing modeling patterns is proposed in Section 6. Section 7 is devoted to show the experimental studies we conducted via modeling patterns. Eventually, Section 8 concludes this work.

2. Related works

In the RAMS (Reliability, Availability, Maintainability, and Safety) domain, patterns have been discussed [45]. Accident analyses are carried out in traffic domain [46] and industrial plants [47]. These studies apply statistical methods to discover patterns of accident causes. The dependability pattern is proposed in [39]. It is defined as the description of a particular recurring dependability problem that arises in specific contexts and presents a well-proven generic scheme for its solution. Resilience design patterns are raised to meet the demand of extreme-scale high-performance computing systems [48].

From the modeling experience of several aircraft systems using AltaRica Data-Flow language, Safety Architecture Patterns (SAP) are proposed to simplify modeling missions [49]. SAP are component assemblies used to ensure the architecture safety [49]. The application of SAP can be found in the avionics domain [49,50]. Unlike their work [49]: First, we use the AltaRica 3.0 language, which has a different mathematical foundation. Mathematical backgrounds of AltaRica Data-Flow and AltaRica 3.0 are mode automata [51] and guarded transition systems [52], respectively. Second, we propose patterns for modeling SIS in the process industry. However, their work is primarily applied in the aviation industry. Third, they mainly proposed the structured collection of redundancy-based architecture patterns. But we describe the behavioral, flow propagation, and coordination characteristics of SIS with modeling patterns.

In a recent work [53], we propose a set of modeling patterns for production-performance analysis. We apply these modeling patterns on a practical offshore installation. The two sets of modeling patterns (in [53] and this article) share some patterns, i.e. CorrectiveMaintenance, SERIES, PARALLEL, and KooN. However, most patterns are different, such as the ad hoc patterns for performance analysis of production systems and patterns for reliability assessment of SIS.

Few studies related to patterns of SIS have been conducted. Related works can be found in [10,54], where the Reliability Block Diagram (RBD) driven Petri Nets (PN) are proposed for reliability analyses. The readability of PN is improved by means of RBD. FT patterns are proposed to model safety mechanisms of automotive electric and electronic functions [55]. FT patterns include second order Safety Mechanisms (SM2) representation, maintenance, periodic tests, and the scenario without SM2.

3. Safety instrumented systems in ISO/TR 12489

We choose the SIS in ISO/TR 12489 as running examples. This is because these architectures are general enough to cover most safety systems [10]. In addition, these systems are representatives of most reliability studies of SIS performed in petroleum, petrochemical, and natural gas industries as well as in other industries [10].

Three assumptions have been made for all systems in ISO/TR 12489:

- Detected and undetected dangerous failures of a given component are independent, with exception of systems #3-2 and #3-3.
- Failure rates are constant.
- Components are as good as new after repairs.

In the following, we recall the SIS in ISO/TR 12489.

3.1. System #1: an overpressure protection system with a single channel

A basic architecture of a SIS is illustrated in Fig. 1. It is composed of a pressure sensor (S), a logic solver (LS), and an isolation valve (V). This system is applied for common safety loops with low to moderate reliability requirements (Safety Integrity Level: SIL1 to SIL2). When the pressure exceeds the predefined threshold, the sensor sends a signal to the logic solver, which in turn commands the isolation valve to close. According to different assumptions, there are four SIS generated from the system in Fig. 1. They are enumerated from #1-1 to #1-4.

The assumptions made for system #1-1 are:

- Periodic tests are perfect and performed simultaneously.
- Installation (protected section) is stopped during repairs and periodic tests.

The assumptions applied for system #1-2 are identical to system #1-1 except that:

- Periodic tests of components are not performed with the same interval.
- Two kinds of periodic tests are performed on the isolation valve:
  - Partial stroking tests to check if the valve is able to move or not;
  - Full stroking tests to check if the valve is tight after closure.

The assumptions assigned for system #1-3 are the same as #1-1 except that:

- The installation is not shut down during the repair of the sensor and of the logic solver.
- The sensor is periodically tested offline. It is no longer available for its safety function during the periodic test.

The assumptions made for system #1-4 are the same as for #1-1, except that coverages of the periodic tests are not 100%. This means that part of the Dangerous Undetected (DU) failure is not covered by periodic tests, and therefore cannot be detected.