Reliability Engineering and System Safety 142 (2015) 456–462

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Fault tolerant design of a field data modular readout architecture for railway applications

Ada Fort [a], Marco Mugnaini [a,*], Valerio Vignoli [a], Vittorio Gaggii [b], Moreno Pieralli [b]

[a] Department of Information Engineering and Mathematics, University of Siena, Siena, Italy
[b] Comesa SrL, Prato, Italy

ARTICLE INFO

Article history:
Received 27 January 2015
Received in revised form
21 May 2015
Accepted 11 June 2015
Available online 20 June 2015

Keywords:
Field Sensors
SIL
Safety design
System availability

ABSTRACT

Modern data acquisition systems used to collect sensor signals are usually designed taking into consideration performance and operating parameters which are mainly related to sensitivity, selectivity, resolution and stability over time. In addition to such important features, field application systems should also respond to other constraints like reliability and availability and additionally, depending on the specific application, to some peculiar requirements in terms of safety. The present paper is addressed to supply an overview of the implications, during a sensor input/output hardware module design, of such parameters as the safety integrity level. The discussion involves the overall system design once integrated with availability considerations. In this manuscript, considerations concerning the on board software implementation are omitted without loss in generality. The study has been developed taking into account solutions suitable for railway applications like signaling or crossing detection systems.

1. Introduction

The design of a sensor acquisition system able to operate in harsh environments and responding to severe constraints in terms not only of data acquisition performance parameters, but also in terms of robustness to common use, is still an open research field. This is due to the fact that, even if compact field distributed acquisition systems are used in a wide variety of industrial contexts ranging from telecommunications up to oil field monitoring ones, safety requirements result to be, most of times, application dependent. In particular in railway signaling systems, for example, the constraints according to some standards [1,2] can represent an actual obstacle for designers both in terms of software and hardware because the safety functions are considered to operate continuously and not only in low demand mode [1]. The introduction of new technologies and new hardware solutions to cover safety functions, even if from one side is an added resource for designers, on the other hand constitutes another constraint. The reason is that usually well proven architectures are a must to comply with the most used standards, avoiding additional testing costs.

Therefore additional design parameters as system reliability, availability maintainability and safety (RAMS) should be considered during the main design phases to ensure that the newly designed system could withstand a wide variety of application conditions. Some researchers have tried to discuss the variation of the system availability and reliability over time for some specific uses related to railways or telecommunications [3–7] or to oil and gas systems [8,9] with only limited safety considerations. These works can in general describe how RAM parameters can change dynamically providing exploitable reconfigurable models. Other authors as in [9–11] tried to describe suitable roadmaps for the definition of degradation models of the systems, trying to keep the safety requirements constrained within upper and lower boundaries. Nevertheless, in these cases authors generally provide complex approaches which may result difficult to be followed by designers in practical approaches where also maintenance considerations should be taken into account. The introduction of advanced techniques as the Hidden Markov Modeling approaches allowed for the embedding of the service shop activities to retrofit the a priori assumed failure and repair rates. In this way, the model is bended to the actual system life under effective use. Such effort in principle is useful to allow system parameter retrofit. Other authors try, as in [12] to show how variations in the risk reduction factor (RRFs) may affect the design options, and try to introduce a rough cost model to discriminate between the options on cost basis. In [13] authors provide an effective approach toward the functional safety assessment of pre-crash systems for reciprocal hazards in the automobile application field building suitable simulation models. Finally in [14,15] authors try to discuss general

* Corresponding author.
E-mail addresses: mugnaini@dii.unisi.it (M. Mugnaini), moreno.pieralli@comesa.prato.it (M. Pieralli).

http://dx.doi.org/10.1016/j.ress.2015.06.008
0951-8320/

approach strategies to address safety problems exploiting traditional methods. Nevertheless, none of the previously mentioned papers address the issue of designing a flexible structure in terms of hardware structure or architecture for sensors readout in order to be able to cope with different safety requirements (linked to different safety functions) with a single modular solution.

Some other authors [16] have discussed the case of safe instrumented systems for low demand mode analyzing the impact of different testing strategies exploited in mechanical and industrial plants. The authors of [17] propose an interesting and simplified method for safety integrity level evaluation based on reliability block diagram degradation approach. Such approach simplifies the formulas presented in [1,2] supplying the designers with a useful tool to be exploited during system design. Nevertheless, this kind of researches, even if introducing alternative approaches to formulas provided into the mostly used standards, has been applied in cases managed with long period of testing proof intervals only and cannot be exploited for continuous operation mode cases. In general case studies [18,19] the designers and researchers focusses most of times in efficiency management and measurement performance skipping most of the considerations on safety constraints introduced by the specific application requirements. Some authors tried to address the problem of analyzing the behavior of low demand mode versus high demand mode systems in terms of both testing proof interval changes and configuration management [20,21]. In particular while [20] focused on the effectiveness of testing on a general instrumented system on the basis of the demand mode classification, [21] tried to optimize the testing proof interval according to a specific selected architecture. Nevertheless neither of these latter [20,21] addressed specifically problems related to railways context which are very peculiar and strictly application dependent.

The authors of this manuscript present an analysis performed within the boundaries of some relevant international safety standards [1,2] to suggest one solution suitable for exploitation whenever an a priori safety design requirement is established.

In details, in this paper the authors tried to start from a basic architecture composed by the sensing element, a logical unit devoted to data manipulation and management, and a final actuating/output element to develop a modular solution able to cope with a commonly required safety integrity level (SIL according to [2] standard), established in particular for railway applications. In these latter cases in particular safety requirements are generally selected according to [1,2] with higher rank (SIL 3 or 4) than in other fields. The proposed modular solutions have been then evaluated in terms of availability parameters, and the best configuration in terms of such parameters has been proposed. The purpose and the novelty of this manuscript resides in the possibility to provide a useful guidance for designers who have to deal with continuous monitoring systems starting from very simple architectures up to complex structures exploitable in particular for railway applications, where standard configurations can be exploited and further enhanced for specific signaling interfacing systems.

The paper is arranged in six sections. In the Section 1 a general introduction to the problem is supplied with an indication of the state of the art of the hardware safety design approaches in different application fields. In Section 2 a general system description and overview is commented. In Section 3 a selected architecture is proposed and different basic configurations are compared in terms of RAMS characteristics, excluding maintenance policies dissertation and assuming only corrective actions. In Section 4 the simulation results are shown and discussed while in Section 5 a possible modular hardware solution able to cover different safety function requirements is proposed. Results in particular highlight that complex system of course may present lower reliability/availability data while proving at the same time a satisfactory protection degree and reduced residual risk. In Section 6 the conclusions are presented.

2. System description

The proposed basic architecture is a fault tolerant smart front end system for safety-critical applications in industrial processes or railway area, supporting severe requirements of configurations and response time. The system works with centralized and distributed configurations, with a modular redundant (MR) architecture to eliminate single points of failure and to ensure the required system availability.

The system can operate correctly with the presence of a major component fault and tolerates multiple, non-concurrent faults if properly arranged in a *XooY* configuration, where *X* is the minimum required number of signals to be received from sensors (inputs), and *Y* is the total amount of available ones. In redundant configurations it identifies and compensates faulty elements and allows for repair activities while continuing an assigned task without process interruption. The system with MR architecture operates as a single set of hardware and software (even if the software section is not discussed in this manuscript and recalled only for diagnosis purposes). The general system architecture can be the one depicted in Fig. 1.

Regarding the system Scan Time, a specific SET-PLC system should be always be present for allowing the selection of the optimal strategy used for elaborating the I/O data. The following three sample different strategies can be applied:

- Polling driven by Main Processor Module
- Spontaneous dispatch at time out
- Data change dispatch

The cycle time between input state change and output state change, e.g. for 1 km communication channel length and 32 I/O module, can be evaluated from 6 ms to 70 ms as typical values depending the strategy used for collecting and elaborating the data.

3. Architectures modeling

Once the basic structure is set, the problem is to define the redundancy of the three main sections of Fig. 1 in order to meet the requirements of multiple safety functions usually present in such systems. The analysis of suitable configurations is developed to meet the requirements of the IEC61508 [2] safety standard (safety integrity level SIL) in designing local or distributed systems for data collection from filed sensors and subsequent manipulation for control purposes. The design will take into consideration the implementation of at least a SIL 3 fault tolerant structures considering the base chain of every safety function as per Fig. 1 due to the fact that this specific application, even if representing a general purpose one, can be specifically exploited for railway signaling monitoring. The possibility to exploit a general structure

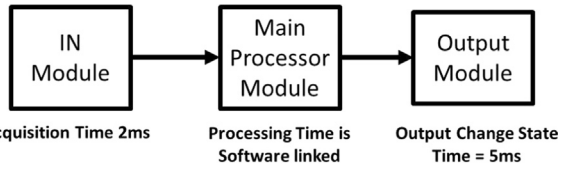

Fig. 1. Basic system description. Acquisition and change state times are assumed as typical mean values for railways cases.