Reliability Engineering and System Safety 155 (2016) 105–114

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

From extended integrity monitoring to the safety evaluation of satellite-based localisation system

Cyril Legrand [a,b,c,*], Julie Beugin [a,b], Juliette Marais [a,b], Blaise Conrard [a,d], El-Miloudi El-Koursi [a,b], Marion Berbineau [a,b]

[a] Univ Lille Nord de France, F-59000 Lille, France
[b] IFSTTAR, COSYS, ESTAS, F-59650 Villeneuve d'Ascq, France
[c] Institut de Recherche Technologique Railenium, F-59300, Famars, France
[d] CRIStAL, UMR 9189, F-59650 Villeneuve d'Ascq, France

ARTICLE INFO

Article history:
Received 1 October 2015
Accepted 20 April 2016
Available online 30 April 2016

Keywords:
Satellite-based localisation system
Integrity monitoring
Safety
Railway safety-related applications

ABSTRACT

Global Navigation Satellite Systems (GNSS) such as GPS, already used in aeronautics for safety-related applications, can play a major role in railway safety by allowing a train to locate itself safely. However, in order to implement this positioning solution in any embedded system, its performances must be evaluated according to railway standards. The evaluation of GNSS performances is not based on the same attributes class than RAMS evaluation. Face to these diffculties, we propose to express the integrity attribute, performance of satellite-based localisation. This attribute comes from aeronautical standards and for a hybridised GNSS with inertial system. To achieve this objective, the integrity attribute must be extended to this kind of system and algorithms initially devoted to GNSS integrity monitoring only must be adapted. Thereafter, the formalisation of this integrity attribute permits us to analyse the safety quantitatively through the probabilities of integrity risk and wrong-side failure. In this paper, after an introductory discussion about the use of localisation systems in railway safety context together with integrity issues, a particular integrity monitoring is proposed and described. The detection events of this algorithm permit us to conclude about safety level of satellite-based localisation system.

1. Introduction

GNSS are usually used in air and road transport for non-safety-relevant applications (fleet management, driver assistance, etc…). In these use cases, the quality of the localisation information is not called into question: the performances provided are sufficient. However, the railway standards [1–3] require a RAMS evaluation for safety-related application like train control and signalling. In other words, before obtaining the authorisation of service, an equipment has to produce a safety documentation conformed to these standards. This documentation describes the degree of confidence that the user can place in the delivered service is needed for the establishment of a safety documentation in order to put the satellite-based train localisation into service. Since the 2000s several projects (LOCOPROL [4], and GIRASOLE [5]) demonstrated that a GNSS standalone receiver is not able to provide a safe navigation solution, particularly in urban and forest area where GNSS signals are subject to multipath effects [6]. As classically done in robotics or other vehicular applications, some of these railway consortia (GADEROS [7], GaLoROI [8] or 3inSat [9]) developed hybridised GNSS-based multi sensor systems based on different choice of sensors and different strategies to ensure safety but exploiting the advantages and drawbacks of each sensor used.

However, GNSS performances are evaluated in terms of another class of attributes (accuracy, availability, continuity and integrity) [10,11] and not in RAMS attributes. In the following part, we propose to focus on the integrity attribute because, in the aeronautic domain, this attribute is well defined and several data processing systems exist to evaluate it (for example, the RAIM (Receiver Autonomous Integrity Monitoring) algorithms [12]). In railways, dependability tools and methods are few for RAMS assessment of GNSS [13] and we propose to counterbalance this observation by revision of integrity (definition and tools) in order to evaluate the safety of these systems.

After describing the satellite-based localisation principles in a literature review, the second part of this paper lays the definition of a performance criterion, the integrity and its monitoring issues. The third section presents the theory about extended integrity for a GNSS/INS localisation train system and its proposed monitoring.

* Corresponding author at: IFSTTAR, COSYS, ESTAS, F-59650 Villeneuve d'Ascq, France.
E-mail address: cyril.legrand@ifsttar.fr (C. Legrand).

http://dx.doi.org/10.1016/j.ress.2016.04.011
0951-8320/

At the end of this section, safety evaluation of our system is done through the extended integrity. The fourth part is devoted to results about, in the one hand, our integrity monitoring algorithm performances and, in the other hand, a safety quantitative analysis of the system. The last section is reserved to conclusions.

2. Literature review: Integrity of a satellite-based localisation system

Before presenting our method to evaluate the safety of a satellite-based localisation system and the proposed integrity monitoring algorithm, some concepts must be explained for the understanding of the proposed solutions.

2.1. Railway embedded systems for localisation: current and envisaged systems

This subsection is dedicated to the state-of-the-art in several localisation systems and particularly for railway (odometer) until we discuss about a solution based on a hybridised GNSS with a inertial system.

2.1.1. Classical localisation systems for dead reckoning

Principles: Dead reckoning is a computation process of the current position by using a previously determined position. In other words, dead reckoning measures the distance and the direction travelled [14]. The *Inertial Navigation Systems* (INS) and odometer are the most used of navigation systems for dead reckoning. These systems are composed of two hardware and software parts and provide a navigation solution i.e. position, speed and acceleration (cf Fig. 1). The acceleration is determined by the measurement of the specific force (f) and angular rate (w) in body frame (roll, pitch and yaw). The hardware part corresponds to the sensor part called *Inertial Measurement Unit* (IMU), which is composed of three accelerometers providing an acceleration measurement and three gyroscopes providing a rotation (angular position) measurement (one for each axis in a inertial frame). The software part corresponds to a computer unit, which resolves inertial equations in order to give a navigation solution. At this level, the measurements coming from accelerometers and gyroscopes are merged. Secondly, an odometer is a device fitted on train bogie axles, which provides a distance travelled by a vehicle. Classically, it is composed of an incremental encoder, which measures elementary motions of the vehicle in the form of impulses (cf Fig. 2). These impulses are converted by a software unit in order to provide a distance travelled.

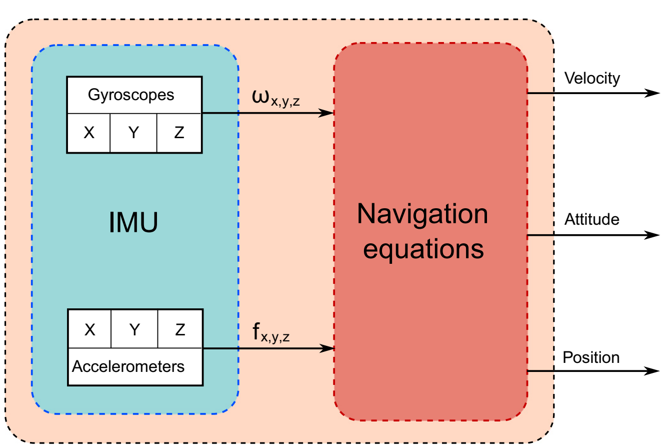

Fig. 1. Inertial navigation system.

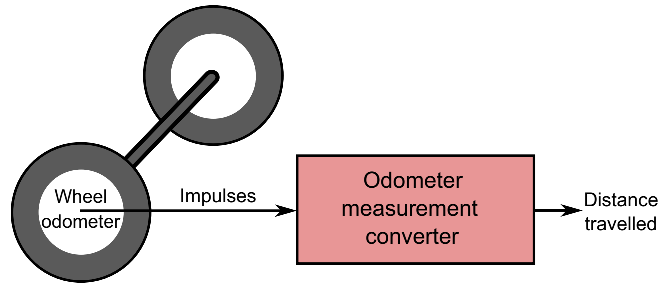

Fig. 2. Railway odometer.

Risks: These systems suffer from slipping phenomena (odometer), gyroscope bias and initial error (INS), which lead to cumulative positioning errors (cf Fig. 3). Further, these positioning errors are called Slowly Growing Errors (SGE) showing the slow and insidious nature of these errors. At their occurrence, SGE are not enough significant to be detected. Without calibration means (note that, in railway context, this calibration is performed by balises, device regularly placed on a railway track), these SGE become too high to be tolerated for missions lasting several hours.

2.1.2. Satellite localisation system

In Europe, existing train control systems are limited to an given territory (a country or a part of a country). Therefore, these systems are all incompatible between them. The on-board equipment and the infrastructure differ from a country to another, which generates interoperability problems. That is why, ERTMS (for European Railway Train Management System), particularly, the ETCS (for European Train Control System) tends towards a new train control system and signalling designed to replace the 27 existing systems in Europe. A GNSS provides a global positioning service thus not limited to a given area. By allowing the reduction of the number of balises along the track, the satellite technology can contribute to reduce the costs of the infrastructure (for example, the balise that can be removed) and to enhance the performances of the ETCS odometry in new trains without impact on equipped lines.

Principles: To locate any vehicle on earth, three satellite signals are required, one for each component of a position in Cartesian system (three unknowns: x, y and z). A receiver measures the range to each satellite, knowing their location. A range is obtained by measuring the transmission time of a satellite signal and the position of this satellite. By using spheres of a radius equal to a range drawn around satellites, two points are given by their intersection, one in space (automatically excluded) and another one on earth (the only one possible for terrestrial vehicle). This calculation is called trilateration. However, the clocks in receivers and satellites are not synchronised. Offsets exist due to relativist effects and delays (a fourth unknown). In consequence, four satellites are necessary to calculate a navigation solution in 3D. The consideration of the clock offsets leads to the computation of pseudo-ranges, written by

$$\rho_u^s = r_{s,u} + (\delta t_u - \delta t_s)c \tag{1}$$

where ρ_u^s is the pseudo-range from a satellite s to an user receiver u, $r_{s,u}$ is the range from a satellite s to an user receiver u, δt_u, δt_s, respectively the clock offsets from user receiver u and satellite s and c, celerity of light.

Risks: GNSS standalone receiver performance is sufficient in open sky areas and for middle density line [15]. However, for terrestrial applications, a navigation solution suffers from several phenomena, which lead to unacceptable errors (sometimes called biases) particularly according to safety and availability point of view. GNSS signals can be reflected by close environment