GRAIL: GNSS Introduction in the RAIL sector

Safety Analysis

Issue	1.0	Date	08/08/2007
Number of pages	43	Classification	PUB

Document Reference

Project	Work package	Partner	Nature	Number
GRAIL	WP3	RSB	DEL	3.4.1

Partner reference (optional)
Gr15my7v6

Responsible	Name/Company	Signature	Date
Author	Martyn THOMAS / RSSB		3/08/07
WP Leader	M.J.García / TIFSA		3/08/07
Project coordinator	A.Urech / INECO		3/08/07
GSA Project Officer	Stefano Scarda		31/07/07

Project funded by the European GNSS Supervisory Authority
6FP 2nd Call. Area 1A: User Segment, User Community
Contract: GJU/05/2409/CTR/GRAIL

DOCUMENT CHANGE LOG

Issue	Date	Affected Sections	Comments
0.1	TBD	All	First draft
0.2	31-May-07	All	Second draft
0.3	11-June-07	All	Third Draft
0.4	15-June-07	All	Re-arrangement of annexes
0.5	20-June-07	All	Final draft after coordinator review
0.6	3-August-07	All	Revision following GSA review
1.0	8-August-07	All	First approved version

DOCUMENT DISTRIBUTION

To/cc	Organisation	Name
To	GSA	Stefano Scarda
To	INECO	Alvaro Urech
To	TIFSA	Mª José García
To	ANSALDO-CSEE	Celso Prados
To	ALSTOM	Michel Rousseau
To	SIEMENS	Klaus Jaschke
To	DIMETRONIC	Beatriz Muñoz
To	THALES	Karl Brocke
To	BOMBARDIER	Georg Mandelka
To	THALES ALENIA SPACE	Lucio Foglia
To	CEDEX	Daniel Molina
To	RSSB	Martyn Thomas
To	DLR	Michael Meyer zu Hoerste
Cc	ADIF	Javier Vicente
Cc	Deimos Space	Antonio Fernández
Cc	ESSP	Umberto Guida
Cc	ESYS	Bryan Jenkins
Cc	IIASL	Frans von der Dunk
Cc	Indra Espacio	Carlos Álvarez
Cc	NSL	William Roberts

TABLE OF CONTENTS

ANNEXES

LIST OF FIGURES

1 INTRODUCTION

1.1 Purpose

This document sets out the safety requirements for the use of GNSS in the following applications to enhance the use of the European Rail Traffic Management System:

- Enhanced Odometry
- Absolute Positioning
- Cold Movement Detection and Train awakening
- Train integrity

The safety requirements describe the hazards associated with these applications, consider the risks and recommends their corresponding integrity requirements. This document does not describe specific mitigations of the risks associated with these hazards, nor does it recommend specific User Terminal design.

As this version of the document constitutes the first release of the document, it reflects the status of the work at the moment of its release. The final version of the document with the full conclusions of the Safety Analysis shall be released at the end of the project.

1.2 Intended audience / Classification

This document is public. It is addressed to the users of GNSS for the applications addressed above and to the designers of a User Terminal intended for these applications. It is the users' responsibility to verify that the context and requirements of his application do in fact correspond to the work presented in this document.

1.3 Associated documentation

This document forms part of the set of specifications produced in WP3 of GRAIL. It complements the application sub-system specifications which are contained in the deliverables D3.1.1, D3.1.2, D3.2.1, D3.2.2, D3.3.1, D3.3.2.

References:

[1] GRAIL-WP3-RSB-MGT-01v1.3 Task 3.4 Work Plan.

[2] GRAIL-WP2-RSB-TEC-01v2.1 Safety Plan

[3] CENELEC EN 50126:1999 Railway Applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).

[4] CENELEC EN 50128:2001 Railway Applications - Communications, signalling and processing systems - Software for railway control and protection systems.

[5] CENELEC EN 50129:2003 Railway Applications - Communications, signalling and processing systems - Safety related electronic systems for signalling.

[6] IEC 1025:1990 part 7 Reliability of systems, equipment and components - Guide to Fault Tree Analysis.

[7] CENELEC EN 60812 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA).

[8] IEC 61882:2001 Hazard and operability studies - Application guide.

[9] UNISIG ETCS SUBSET-026 ETCS System requirements Specification

[10] UNISIG ETCS SUBSET-036 FFFIS for Eurobalise

[11] UNISIG ETCS SUBSET-078 ETCS FMEA RBC-RBC Handover

[12] UNISIG ETCS SUBSET-079 ETCS FMEA MMI

[13] UNISIG ETCS SUBSET-080 ETCS FMEA TIU

[14] UNISIG ETCS SUBSET-081 ETCS FMEA Transmission Path FMEA

[15] UNISIG ETCS SUBSET-088 ETCS Application Levels 1 & 2 - Safety Analysis

[16] UNISIG ETCS SUBSET-091 ETCS Levels 1 & 2 Safety Requirements for Technical Interoperability.

[17] Galileo Mission Requirements Document (MRD) issue 6.

[18] GRAIL-WP2-RSB-DEL-2.1.1 Safety Applications and the Requirements Background

1.4 Abbreviations and Acronyms

DRM	Digital Route Map
EGNOS	European Geostationary Navigation Overlay System
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
FMEA	Failure Modes and Effects Analysis
GSA	Galileo Supervisory Authority
HAZOP	Hazard and Operability studies
IHA	Interface Hazard Analysis
PHA	Preliminary Hazard Analysis
RBC	Radio Block Centre
SHA	System Hazard Analysis
SIL	Safety Integrity Level
SIS	Signal-in-Space
TBD	To Be Defined
THR	Tolerable Hazard Rate
UT	User Terminal
WP	Work Package
WPL	Work Package Leader

1.5 Definitions

Digital Route Map

The digital route map is a data base of the coordinates of the track alignment in two or three dimensions.

Mission time

The period over which a probability or rate of failure applies.

Safety Integrity level

A number which indicates the required degree of confidence that a system will meet its specified safety functions which respect to systematic failures (EN50129-2003).

Radio Block Centre

The term given to the control centre part of ETCS.

Signalling

The information displayed to a train driver that defines at least the limit of his movement authority, and can include warnings when approaching this limit and the permitted speed profile.

Train control system

The system that provides the combined functions of signalling and train protection.

Train protection

The reduction (usually automatic) of a train's speed in response to a measurement indicating that it is at risk of exceeding the limit of the movement authority, and can include the continuous monitoring of speed against limit permissible limit and reverse movement protection.

User Terminal

The equipment that provides the enhanced GRAIL functions to ETCS.

1.6 Document Structure

This document presents the Preliminary Hazard Analysis and the supporting information required by the GRAIL task 3.4 work plan [1]. The work relating to the activities specified is presented principally in the annexes to this document. The main text provides the logical links between these annexes and provides background information where necessary.

2 SUPPORTING INVESTIGATIONS

2.1 Previous Work

Many projects have considered the role of GNSS in railway applications[1]. This report considers the contribution of two recent projects, GADEROS and LOCOPROL, together with the work undertaken within WP2. The basis of the work is described in the Safety Plan [2], which is updated as the work proceeds.

2.1.1 GADEROS

The GADEROS project principally considered the feasibility of the use of GNSS for the purposes of absolute positioning. Part of this work made an initial assessment of the safety issues in the context of ETCS. Since then the documents available from UNISIG have developed significantly and some of the results of this work would require revision. However, those that have retained relevance are summarised here.

The project identified the need to understand the origin of the GNSS performance requirements, especially those which relate to mission time. It will be necessary for the railway applications to work with these and to achieve its requirements through receiver design and augmentation. The report included fault trees that are still relevant and may provide the basis for further work in GRAIL. In addition, the project looked at the consequences of GNSS errors in the context of the dynamics of a railway. There is more progress to be achieved in this area.

2.1.2 LOCOPROL

The LOCOPROL project developed an innovative approach to a GNSS-based vital train signalling system for low traffic lines. On the basis that the global LOCOPROL system requires a tolerable hazard rate (THR) of 10^{-9}/hour (a conventional estimate for the signalling system as a whole) the positioning requirement was set a target tolerable hazard rate of $6*10^{-11}$/hour and the speed calculation a tolerable hazard rate of $6*10^{-10}$/hour. LOCOPROL developed a safety analysis technique based upon pairs of satellites. Making a deliberately pessimistic approach to the accumulation of errors and estimates of the confidence interval in position provided by one pair of satellites, the project suggested safety margins on position of between ±108metres and ±215metres on the estimated position should be possible when 4 satellites (that is two pairs) are in view. The project recommended that further work would confirm that the target THRs are achievable. It presumed the use of GNSS without augmentation, other than EGNOS, and a concept of operations that would ensure that trains would run and the safety properties required only when the satellites are in view (and these are predictable). Also of interest is that within the overall THR, the project suggested that train spacing should be apportioned a THR of between 10^{-10} and 10^{-12}/hour.

2.1.3 GRAIL WORK PACKAGE 2

WP2 undertook three lines of work at the level of system requirement:

An initial assessment of the hazards associated with the safety related applications of GNSS on the railway.

Reviews of the GNSS context and its relationship to applications with safety requirements.

[1] A list that is not exhaustive includes, GILT, GALA, APOLO, ECORAIL, F-MAN, INTEGRAIL, LOCOPROL, LOCOLOC.

A description of RAIM and its use in the context of limited satellite visibility.

The work on RAIM is particularly interesting as it complements the fault trees produced in GADEROS. It underlines the importance of the use of digital route maps and RAIM together, and it indicates a direction for future investigations.

2.2 Summary of the Principles of the Investigation

2.2.1 Objective of the Study

2.2.2.1 The activities reported in this study are based upon the requirements of the International and European standards [3] to [8], applied in the railway domain, the ETCS specifications [9] to [16] and the available knowledge of GNSS [17]. The objective is to set out to the extent possible the safety requirements of the GNSS applications studied, and the contribution to these requirements that should be provided by the User The task 3.4 safety activities consist of a Preliminary Hazard Analysis (PHA). Each application of WP3 addressing the design of the User Terminal sub-system will be the subject of a PHA.

2.2.2 Contents of the Study

2.2.2.1 The safety plan [2] sets out the manner in which the safety requirements will be obtained and managed during the project.

2.2.2.2 The PHA will include:

A model suitable for functional failure analysis

Functional failure analysis

Identification of event sequences leading to unsafe behaviour of ETCS

Identification of barriers able to reduce the likelihood of unsafe behaviour

Risk assessment, quantitative where practicable

Safety Integrity Level recommendation

2.2.2.3 The detailed design of a User Terminal is not in the scope of the PHAs.Terminal.

2.2.2.4 The contents of the task are set out in the work plan [1]. The activities are summarised as:

Activity	**Title**
	WP3.4 Kick off Meeting
1.1	PHA Enhanced odometry
1.2	PHA Absolute Positioning
1.3	PHA Train Awakening/Cold Movement Detection
1.4	PHA Train Integrity
1.5	Review 1.1 to 1.4 if amended.

Activity	Title
2.1	ETCS: safety review of established requirements
2.2	Assessment of railway hazards and risks related to signalling, train detection and train protection
2.3	Use of augmentation
2.4	Use of Digital Map
2.5	The influence of system architectures
2.6	Review of WP4.
2.7	Review of Acceptance Criteria

2.2.3 System Context

a. Figure 1 shows the safety context which is applied to the activities. The objective is to define the safety requirements of the User Terminal such that the applications can safely depend upon GNSS.

Figure 1. The safety context of the GRAIL applications

b. This is applied to the generic location system illustrated by Figure 2.

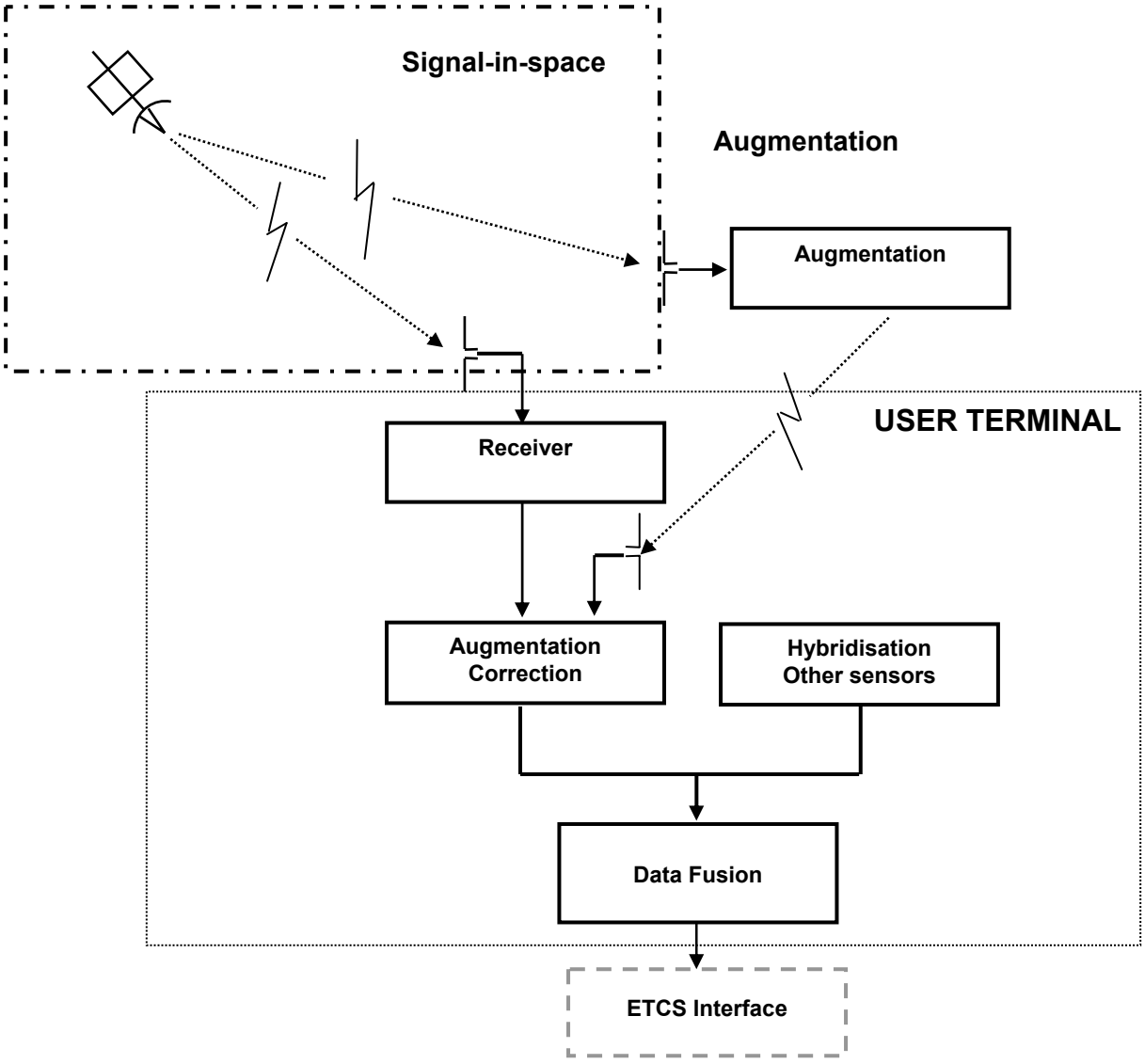

Figure 2. The GRAIL system context

2.2.4 The Principles of Safety

2.2.4.1 Tolerable hazard rate

In these investigations the THR refers to those failures that bring risk of accident and that are not detectable. When detected measures can be taken to control the effects of the failure. Provided these failures are detected and the controls are put in place within a certain period then the risk is considered to be controlled.

When apportioned THR is calculated for the following bounds:

Onboard, a single onboard equipment,

Trackside, the equipment met within a defined mission profile.

The concept of mission profile is defined within the ETCS documents (see below). Another approach that can be applied is that of a macro-representation of a network. This suggests the safety performance of the network as a whole, leaving the specific variations inside the network to the responsibility of the management. Some railways do use targets that represent their network. There may be developments in this direction for Europe as a whole under the Safety Directive 2004/49/EC.

Where GNSS is concerned, there may be a view to be taken on the representation of satellite obscuration due to the nature of the network. For Britain, some work in this direction has started.

2.2.4.2 Safety Integrity Level (SIL)

SILs need to be handled with care. They apply to an application of a given system. They are best interpreted as expressing the degree of dependence that the user places on the system to support the application. As an example of the highest SIL, consider the meaning of a “clear” lineside signal (typically a green aspect) to the driver of a train. He is travelling at 200km/h in a train weighing several hundreds of tons with several hundreds of passengers. He has to have “blind faith”, the expectation, that there is no other train ahead, and that the route ahead is fit for purpose. If he had not this faith he would be driving as if his train were a tram. (As well as this dependence on the signalling, he also depends on other parts of railway operations to ensure that there is no incursion on to the track and that it is otherwise fit for purpose; these matters are not absolutely in the scope of the meaning of the green aspect and this is understood.) The ability of the signalling system to merit this expectation is expressed as its dependability - it is there when it is needed and it means what it says to probability at least as high as the absence of other risks. This level of dependence is expressed as SIL4.

This does not mean that elements of the signalling system have to meet SIL4 requirements. It does mean that the contribution of risk that each element brings cannot bring the dependability into question. In the extreme case, an element may require SIL4 properties, but in the general case the system architecture provides checks such that if a failure does exist it is detected. An example of a SIL4 element is a signalling relay used in an interlocking for switching the signals to the driver. These relays have intrinsic properties such that they cannot remain falsely operated except with a low probability (it has happened due to zinc migration and even insects it is claimed). Relays not with intrinsic safe properties can be used in signalling, and then other measures are taken to detect false operation such as back-proving and more complex interlocking logic. Today, with data processing technologies, the individual components in the data processor (computer) have no safety properties. Yet SIL4 systems are obtained by means of particular architectures and coding techniques.

A similar discussion can be had on train detection, speed and distance measurement. What must be demonstrated in the signalling system is that in normal operation the driver can depend upon the information he is given, and that the risks of any errors in this information, and on his part in acting on this information, are acceptable to society as a whole. Accepting that perfect safety is not possible, governments interpret the view of society as to what constitutes safe operation. The resulting risk is expressed as a THR, which is the basis of the ETCS safety analysis.

Because safety costs money, it is not a reasonable objective to make everything as safe as possible. Resources are finite and are limited. Effort expended in reducing risk in one part of a system or even society reduces the effort available to the other parts. Therefore, as a principle of safety management, the parts of a system that are required to have safety-related characteristics should be the minimum necessary to obtain the required risk control. Anything extra represents a waste of resources.

Where GRAIL is concerned, this means that the contribution of GNSS to the risks of operating ETCS should not increase the overall risks to the public, and must not reduce the dependability of the train control system (defined as the signalling function - giving information to the driver - plus the protection part - mitigating driving errors) in normal railway operating conditions. This means that the User Terminal must be fit to support the SIL4 application, and there will be safety requirements. It does not follow that all these requirements are themselves classified as SIL4.

2.2.4.3 Degraded modes

The above discussion applies to normal running line operations, called Full Supervision in ETCS specifications. When the system is suffering from failures or in other operating circumstances the system operates in a degraded mode, not providing its full functionality. In these cases the role of the User Terminal has to be re-assessed. A notable feature of degraded modes is that the driver necessarily has more responsibility in assuring safety, and the dependence on the ETCS is reduced. In the extreme case where ETCS is not able to contribute to operations the driver and signaller together share responsibility for achieving safety supported by the quality of the procedures that they implement.

2.3 Review of Established ETCS Safety Requirements

2.3.1 The Role of ETCS Protective Functions and Procedures

Lineside signals are considered to provide SIL4 information. To provide SIL4 response to these ETCS includes train protection functions that detect train behaviour that indicate that the driver is not responding to the information safely. The presence of these functions reduces the dependence on the signalling providing that they have SIL4 properties. Although not applicable to lineside aspects, when the information is displayed to the driver in the cab (cab-signalling) the display technology is simplified provided the protection functions of adequate SIL are available. This is the normal situation. When ETCS protective functions are not available, or their SIL is reduced, then the information presented to the driver and the implementation of the operating procedures acquire a more important safety significance. This can justify a display of higher SIL and greater dependence upon location functions that could be provided by the User Terminal, but this study will work within the existing ETCS regime that the degraded procedures include cooperation between driver and signaller that do not place greater dependence upon the display of information to the driver, and therefore the location functions, than in normal service.

2.3.2 EuroLoop

The use of Euroloop is not considered in this study. Where it could be applied its safety performance is assumed to be at least as good as that obtained by the use of balises and the radio communications.

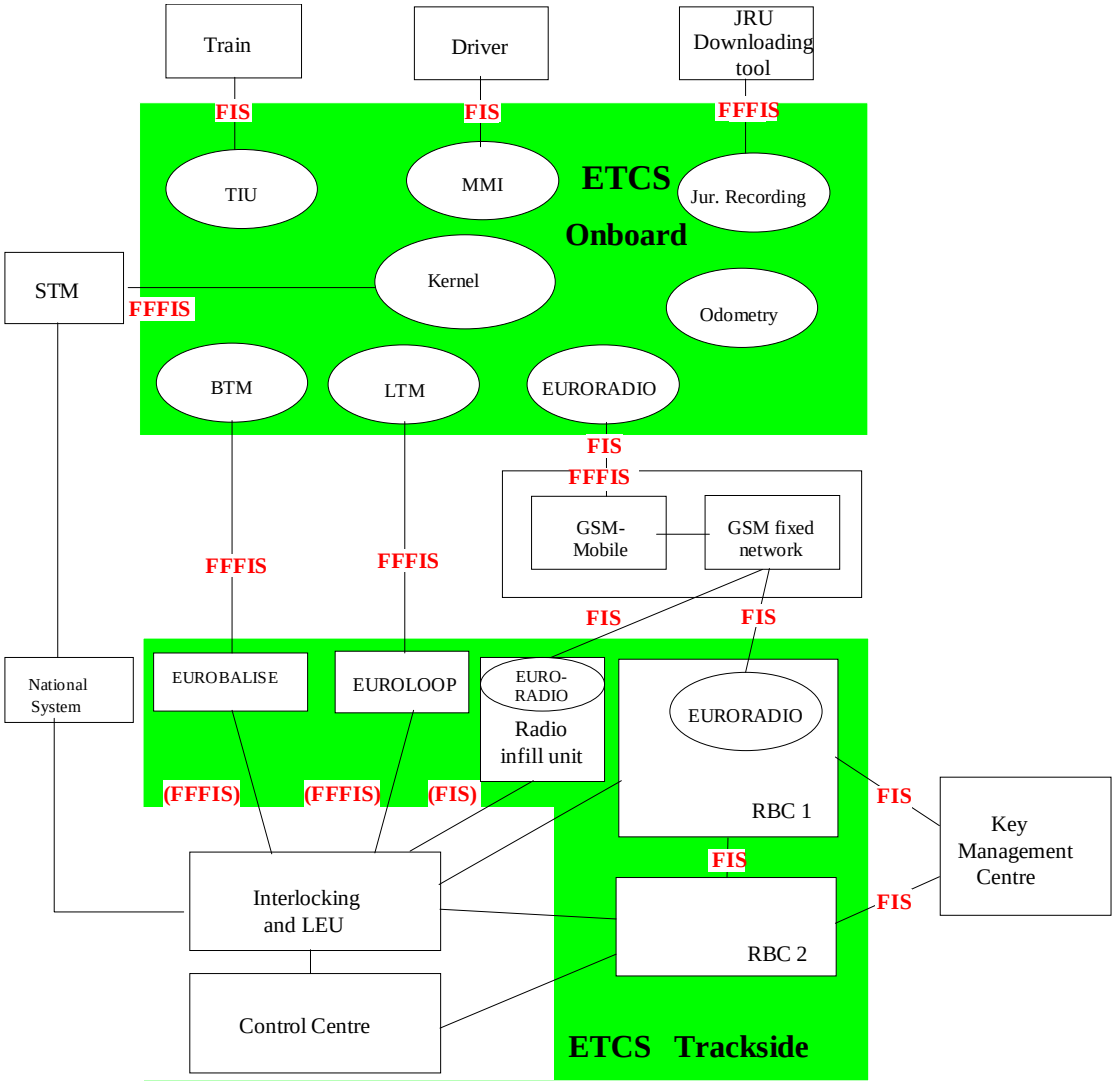

Figure 3. ERTMS/ETCS Reference Architecture

2.3.3 ETCS and the Influence of the Enhanced Functions

Figure 3 (from reference [9]) represents the functional architecture of the ETCS.

The applications studied in GRAIL introduce the opportunity to review sources of potential error and failures in the following ETCS macro-functions:

Time (not shown)
Odometry (Speed and distance)
Spot data transmission (data affecting odometry, cab-signalling and automatic train protection).

The use of GNSS certainly affects the onboard equipment performance, but has a very limited effect upon the trackside equipment. Two possible effects at the trackside are:

1. The use of GNSS time to synchronise the trackside and the onboard systems over a complete network.

2. The reduction in the number of balises (in principle to zero) by the use of a Digital Route Map (DRM).

The use of GNSS in ETCS will introduce hazards that do not exist in the present implementations, and these hazards must be subjected to controls and mitigations so that the overall THR is not worse than that required today. For the purposes of interoperability, a THR for ETCS has been defined, and is apportioned to those parts of it where a consistent performance throughout the European railways must be provided.

2.3.4 The Requirements of the Established ETCS Specifications

ETCS specifications, references [9] to [16] are reviewed to extract those safety requirements which:

1. Any GNSS-based solution must respect because they concern one of the macro-functions identified above,

2. May change because of consequent modifications to the equipment arrangements (for example, less trackside equipment).

The use of GNSS must not change the safety requirements (as expressed as THR) of those “conventional” parts of ETCS required for interoperability, otherwise the achievement of interoperability is threatened. In adding equipment to the onboard part for the purposes of GNSS without compensating influences its THR is necessarily increased. A sub-apportionment of the allowable THR onboard to the GNSS equipment is required for each application. Such compensating influences can be brought about by attention to the overall system architecture, of which the following are examples:

Complementarity between the failures in the GNSS and failures in other parts of ETCS, that is a failure is detected in another part of the system (independence of failures is required).

The reduction in the trackside equipment made possible by certain uses of GNSS permits the THR apportionment to be transferred to the onboard GNSS equipment.

Annex A reports those ETCS requirements in the references that the ETCS enhanced applications must respect. In addition it indicates where GRAIL may have an influence upon the factors that were used in determining those requirements.

2.4 Assessment of Railway Hazards and Risks Related to Signalling, Train detection and Train Protection

Annex B (to be completed in the next issue of this document) sets out the concept of safety that is applied in the railway domain in this document. This is reconciled with the safety concepts that are embodied in the GNSS specifications and the intrinsic properties of these systems. The text below is an introduction to the issues which will be addressed.

Railways do not need signalling. Well, in a perfect world they would not. This statement, fundamental to understanding the role of signalling, is predicated on the following assertions:

A perfect timetable would contain no conflictions between trains
Trains would run to timetable
Switches could be set by timetable
There would be no failures.

The purpose of this discussion is to suggest that the safety demand on signalling and train protection in the operation of the railway is not continuous. Conventionally it has always been assessed as continuous, but rather it assures safety in response to particular events. These occur at a point in time, and only a limited time is available before the railway must be brought back to a state of safety. The conventional signalling technology provides a consistent behaviour almost independent of time. The use of GNSS provides an opportunity to review this approach to the demonstration of safety. A particular feature of the safety performance of GNSS as it is specified is the concept of mission time, and the probability of a hazard occurring within this period

The behaviour of GNSS is not an absolute. It is determinate within limits that are a function of the unknowns within the system; examples of these are the precision with which the orbits of the satellites are known, the behaviour of the radio waves in the atmosphere, the effects of multipath, the geometric arrangement of the satellites in view. The specifications for performance of GNSS recognise the statistical behaviour of GNSS, and they are formulated principally in response to the requirements of the aviation sector. Pragmatically, the basic safety behaviour of GNSS is one to which the railways must adapt if possible. Where it can be demonstrated that this is inadequate for the needs of the railways then augmentation to the GNSS can be specified with the necessary safety characteristics. Annex B sets out the basic safety properties of the railway and places these into the context of the aviation requirements on GNSS.

The starting point is to describe the nature of risk on the railway. Normally the railway is in a safe condition. The questions arise, if a risk to safety arises at a point in time, how long does it take for the circumstances which could lead to an accident to be created? And for how long after the incident is the GNSS required to be dependable? Each GRAIL application is considered in turn.

2.4.1 Enhanced Odometry

The cases to be considered are:

1. where conventional track based train detection is in use, there are two sub-cases:
   a. Lineside signalling, in this case the User Terminal is used by the train protection functions, not signalling.

      Discussion.

      Where level 1 is being applied and real balises are in use, the application of the User Terminal is limited to measurement of speed and position so that if overspeed is detected ETCS can invoke intervention. In this case, a DRM if used, does not replace real balises. The DRM participates in the location function only. The

driver's information from the signals is independent of the data channels used to invoke intervention.

The time for a train to come to rest after intervention generally is less than 150 seconds. After intervention, there is no speed or position control function and the brakes remain fully applied. There is however an optional brake release function which operates when the train comes within the safe speed envelope. Level 1 applied with a DRM without real balises is treated under Absolute Positioning.

b. Cab-signalling, in this case the User Terminal contributes to the display of information to the driver and the protection functions, but does not affect the interlocking part of the signalling system.

Discussion

The display to the driver is effectively a profile of speed against distance. If the User Terminal's measured train's position causes the display to indicate a higher target speed than it should, this is likely also to be reflected in the intervention curve because the display and the protection functions share the same data channel. This is the case to be analysed.

However, the independent train detection ensures that the interlocking cannot be affected by User Terminal errors.

2. where the User Terminal is used both for signalling (separation from point of danger and display to the driver) as well as protection functions. This is known as ETCS level 3.

Discussion

ETCS level 3 is largely undefined. Although it is promoted as being without track-based train detection, there are many open points including the practical extent to which track-based train detection can be dispensed with, for example in points and crossings and at level crossings. If used with real balises and radio data transmission the GNSS may invoke changes to the safety context, but these are trivial compared with the fundamental issues surrounding level 3. A deeper discussion is included with absolute positioning.

2.4.2 Absolute Positioning

1. Where conventional track based train detection is in use, there are two sub-cases:

a. Lineside signalling, in this case the User Terminal is used by the train protection functions, not signalling,

Discussion

Where level 1 is being applied and a DRM is in use, the User Terminal:

- *uses the train's measured position to extract data from the DRM*
- *measures speed and position so that if overspeed is detected ETCS can invoke intervention. The driver's information from the signals is independent of the data channels used to invoke intervention.*

The absence of balises means that there is no independent reference with which to detect position errors. The data in the DRM will be applied with the prevailing error in the position measurement. Intervention will also be similarly affected.

The time for a train to come to rest on average after intervention is less than 150 seconds. After intervention, there is no speed or position control function and the

brakes remain fully applied. There is however an optional brake release function which operates when the train comes within the safe speed envelope.

b. Cab-signalling, in this case the User Terminal contributes to the display of information to the driver and the protection functions, but does not affect the interlocking part of the signalling system.

Discussion

The display to the driver is effectively a profile of speed against distance. If the User Terminal's measured train's position causes the display to indicate a higher target speed than it should, this is likely also to be reflected in the intervention curve because the display and the protection functions share the same data channel. This is the case to be analysed.

However, the independent train detection ensures that the interlocking cannot be affected by User Terminal errors.

The absence of balises means that there is no independent reference with which to detect position errors. The data in the DRM will be applied with the prevailing error in the position measurement. Intervention will also be similarly affected.

The time for a train to come to rest on average after intervention is less than 150 seconds. After intervention, there is no speed or position control function and the brakes remain fully applied. There is however an optional brake release function which operates when the train comes within the safe speed envelope.

2. Where the User Terminal is used both for signalling (separation from point of danger and display to the driver) as well as protection functions. This is known as ETCS level 3.

In this case, a DRM is essential. The DRM participates in the location function and referencing the data applicable at that location. As stated under enhanced odometry, level 3 ETCS is largely undefined outside of the concept of minimising track-based train detection. The User Terminal data is used for the driver's display, the protection functions and at least some of the interlocking functions.

Discussion

Analysis of this application will identify the full range of the relationship between User Terminal errors and the railway. This will be undertaken for the final deliverable. It may not be possible to address all level 3 issues.

2.4.3 Cold Movement Detection and Train Awakening

This application concerns only position and train orientation. In addition it has the particularity that it is an application that has time for the location to settle over several minutes. It should be specified what this duration is, and it remains to be determined whether this gives a finite advantage. It is the most demanding application in terms of accuracy.

In this case, a DRM if used does not replace real balises. The DRM participates in the location function only. The advantages given by a DRM when a train is moving (anticipating radius of curvature, detecting turnouts) of course are not relevant, but when a restricted number of satellites are available it will probably prove to be beneficial.

The extended time available for a position means that this discussion is not relevant to this application.

2.4.4 Train Integrity

This application concerns only position. It has the particularity that the locator at the tail is subsidiary to the locator at the head. No challenging accuracy is required; even margins of 50 metres would give a performance superior to that which is possible today. The control of tolerances is aided by the assumption that the tail of the train is on the same signalled route as its head, and it is reasonable to consider that errors detected at the head of the train can largely be applied to the tail. A fast detection of train separation is not required. Obviously the faster the better, but in terms of conventional signalling, there is protection, but actually detecting a divided train can take some time. Its use in ETCS level 2 is a convenience, but not a necessity for safety, however at level 3 it is a necessity.

The extended time available for a location means that this discussion is not relevant to this application.

3 SUPPORTING GNSS STUDIES

3.1 Introduction to Satellite Navigation for Railways

GNSS is extensively applied in the aviation and maritime sectors. Both place an emphasis on safety, but the former is probably the origin of the standards in place. The following concepts are used;

Accuracy. This is a statistical concept. When specifying a GNSS positioning accuracy it is essential to specify the statistical context. In this document, it is assumed to be Gaussian, and a reference to standard deviation is included with statements of accuracy.

Integrity. This is the ability of a system to provide timely warnings when the system should not be used for safety purposes.

Integrity Risk. GNSSs are able to assess with a defined probability the errors present in the measured navigation parameters. When the errors exceed a defined threshold an alarm is triggered, within a specified period. Integrity Risk is the probability that an error remains undetected for longer than this period. In the aviation domain, this probability is expressed as a tolerable hazard rate that is achieved within a defined period. This period corresponds to the mission time.

Mission time. This is the period during which a demand to preserve safety has to be made upon the system that is depending upon the GNSS. In this period a specified certainty of success or dependability (that is: 1-probability of failure) is required. There is a need to define this period in the context of the railways (see annex B).

Time-to-alarm. This is the maximum allowable time between an alarm condition occurrng in the Signal-in-space, and the alarm made available to the user. There is a need to define this period in the context of the railways.

3.1.1 GNSS Augmentation

The basic GNSS system provides range and speed information that is derived from the data describing the geometry relating the position of the receiver to the ephemeris of the satellites. This data is subject to errors that can be reduced by augmentation techniques.

3.1.1.1 Wide area augmentation

Wide area augmentation is the technique where the errors in the data received from the satellite are assessed at a point of reception that has been surveyed precisely. The errors are quantified and broadcast to users of the data over the area concerned. The European technique is called EGNOS (European Geostationary Navigation Overlay System). EGNOS is now fully deployed and in its pre-operational phase. The system will undergo certification for safety-of-life applications before becoming fully operational. It is foreseen to enter full service in 2008. The corrections are broadcast to users over a communications link that uses a geostationary satellite system (Inmarsat).

3.1.1.2 Differential GNSS (DGPS)

An alternative to the use of geostationary communication satellites to broadcast corrections is the use of low medium wave frequencies. These propogate well and the usable range is about 100 km. The coverage over coasteal areas is largely complete, and inland areas are being provided with this facility. However, their usefulness in a railway environment could be limited by electro-magnetic interference.

3.1.1.3 Local area augmentation

As the name suggests this facility broadcasts corrections over a smaller geographic extent, perhaps a few kilometres. It has the potential to provide better control of the errors and therefore offer better precision than a wide area solution. However, the means to broadcast the corrections has not yet been normalised. It could be that the needs of the railways encourage this process. .

3.1.2 Receiver Autonomous Integrity Monitoring (RAIM)

Receiver autonomous integrity monitoring (RAIM) is a function in the user's receiver that to a given value of certainty detects inconsistencies in the received data. It ensures that a large proportion of errors and failures whose origins lie outside of the receiver do not go undetected. It uses the redundancy that occurs when the number of satellites in view is more than the strict minimum necessary for a position to be determined.

3.1.3 The Risks in the Absence of Failures

In this document it is assumed that the errors affecting the accuracy of a GNSS-based hybrid odometer are Gaussian in nature. The interpretation to be applied to the term “accuracy” is then based upon the Gaussian distribution. There is a small probability that when all is working to specification that the instantaneous accuracy will be so low as to permit a train to stray beyond the stopping point, beyond the safety margins and beyond the point of danger. Where accuracy is degraded by the performance of one satellite or by the geometric arrangement of the satellites in view, the duration of this situation is limited. However, once this situation has occurred for long enough to disturb the spacing of trains, there is a risk that the error in the train location would cause a dangerous end-of-movement authority to be displayed to the driver. As a consequence the train could be driven beyond the point of danger and train protection would not be effective. The use of augmentation and RAIM are two important means to mitigate the risk that an error would not be detected. Other risk mitigation techniques are possible and will be discussed in the next issue of this document in order to take a view on the risk reduction that must be provided in the User Terminal, as indicated in figure 1.

The formal introduction of GNSS to safety related applications introduces the use of statistical methods to performance estimation to a greater extent than previously. One particular feature of this requires mention. In previous safety analysis on the railway a failure or error is present or it is not. It does not come and go. Probability was assigned to its happening but not its duration. The use of GNSS requires consideration of the duration of a failure or error as well. A failure that lasts for one second is unlikely to have an effect on the railway. A failure that is permanent certainly will have an effect. Somewhere between these two extremes there is a threshold that remains to be defined. The analysis of the duration of errors is a new requirement, and its solution in safety terms presents new questions to be understood by the railway.

Although essential to be considered in the overall design this study excludes consideration of jamming/spoofing (masquerade).

3.1.4 The role of the Onboard Map

The DRM is not currently part of the core ETCS specifications, but there is no formal obstacle to its use. There is also a duality in the ETCS communications architecture, balise and data radio. The

concept of the use of a database in ETCS is not new. At levels 2 and 3 the Radio Block Centre (RBC) depends upon databases describing the railway.

The DRM supplements the use of the balise, but at levels 2 and 3 it also reduces significantly the dependence on the radio communication. This could require a re-assessment of the hazards associated ETCS operations in certain cases.

Safety is a crucial question when considering the use of data bases. It should be noted that one of the possibilities that the DRM introduces is a means to provide a verification of the RBC data against that held on the train. Provided there is some independence between them, this introduces the possibility of some verification of their contents.

3.2 The Influence of System Architectures

Annex C (to be completed in the next issue of this document) sets out the manner in which GNSS can be implemented and discusses the safety influences implicit in each.

3.3 Safety and Augmentation

Annex D (to be completed in the next issue of this document) sets out the failures specifically related to the augmentation of the GNSS signal-in-space (SIS) by EGNOS. It is the intention to consider the safety implications of these failures in the next issue of this document.

3.4 The Use of a Digital Map and Safety

Annex E sets out the benefits to safety and performance that can be provided by the use of a digital route map, and the complementary safety matters that must be addressed.

4 PRELIMINARY HAZARD ACTIVITIES

The Task 3.4 Work Plan ([1]) sets out the activities to be undertaken for each of the sub tasks. These are set out into two groups. Group 1 obtains the safety requirements of the four applications through a process described as a PHA. This is described in [1] as containing the following subjects:

- Model
- Functional failure analyses (HAZOP and FMEA)
- Event sequences
- Barrier identification
- Risk and SIL estimation

This section presents the first and second subjects in order of the application. The remainder are presented in section 5. The HAZOPS were conducted in accordance with the guidance reported in WP2 ([18]). The FMEAs were conducted in accordance with the guidance given in annex F.

Group 2 contains activities that support sections 4 and 5 are reported in section 3 and the end of section 5 where end of project review is involved.

4.1 Enhanced Odometry

4.1.1 HAZOP

The report on the HAZOP conducted on the Enhanced Odometry specifications is given in annex G.

4.1.2 FMEA

The report on the initial FMEA conducted on the Enhanced Odometry specifications is given in annex H together with the results tables.

4.1.3 Hazard Log

The report on the HAZOP conducted on the Enhanced Odometry specifications is included in annex I.

4.2 Absolute Positioning

4.2.1 HAZOP

The report on the HAZOP conducted on the Absolute Positioning specifications is given in annex J.

4.2.2 FMEA

The report on the initial FMEA conducted on the Absolute Positioning specifications is given in annex K together with the results tables.

4.2.3 Hazard Log

The report on the HAZOP conducted on the Absolute Positioning specifications is included in annex I.

4.3 Cold Movement Detection and Train Awakening

4.3.1 HAZOP

The report on the HAZOP conducted on the Cold Movement Detection and Train Awakening specifications is given in annex L.

4.3.2 FMEA

The report on the initial FMEA conducted on the Cold Movement Detection and Train Awakening specifications is given in annex M together with the results tables.

4.3.3 Hazard Log

The report on the HAZOP conducted on the Cold Movement Detection and Train Awakening specifications is included in annex I.

4.4 Train integrity

4.4.1 HAZOP

The report on the HAZOP conducted on the Train Integrity specifications is given in annex N.

4.4.2 FMEA

The report on the initial FMEA conducted on the Train Integrity specifications is given in annex O together with the results tables.

4.4.3 Hazard Log

The report on the HAZOP conducted on the Train Integrity specifications is included in annex I.

5 SIL DETERMINATION AND CONCLUSIONS

This section will be completed in the next issue of this document.

5.1 *Enhanced Odometry*

5.1.1 *Event Sequences and Barrier Models*

5.1.2 *Criticality assessment*

5.1.3 *SIL Recommendation*

5.2 *Absolute Positioning*

5.2.1 *Event Sequences and Barrier Models*

5.2.2 *Criticality assessment*

5.2.3 *SIL Recommendation*

5.3 *Cold Movement Detection and Train Awakening*

5.3.1 *Event Sequences and Barrier Models*

5.3.2 *Criticality assessment*

5.3.3 *SIL Recommendation*

5.4 *Train Integrity*

5.4.1 *Event Sequences and Barrier Models*

5.4.2 *Criticality assessment*

5.4.3 *SIL Recommendation*

5.5 *Review of Acceptance Criteria*

5.6 *Observations relevant to Safety from WP4*

6 CONSOLIDATED REQUIREMENTS FOR ENHANCED ETCS APPLICATIONS

To be completed in the next issue of the document.

END OF MAIN DOCUMENT

Annex A:

Review of Established ETCS Safety Requirements

This document is internal to the GRAIL consortium

Annex B:

Railway Hazards and Risks Related to Signalling, Train Detection and Train Protection

This document is under development

Annex C:

The Influence of System Architectures

This document is under development

Annex D:

EGNOS Failures Study

This document is under development

Annex E:

Improving Accuracy and Integrity in Rail Applications through the Integration of GNSS with a Digital Route Map

This document is public

Annex F:

FMEA for ETCS Applications: Members Information Pack

This document is internal to the GRAIL consortium

Annex G:

HAZOP for ETCS Applications: Enhanced Odometry

This document is internal to the GRAIL consortium

Annex H:

Enhanced Odometry FMEA Report

This document is internal to the GRAIL consortium

Annex I:

The GRAIL Hazard Log
(as at 1 June 2007)

This document is internal to the GRAIL consortium

Annex J:

HAZOP for ETCS Applications: Absolute Positioning

This document is internal to the GRAIL consortium

Annex K:

Absolute Positioning FMEA Report

This document is public

Annex L:

HAZOP for ETCS Applications: Cold Movement Detection & Train Awakening

This document is internal to the GRAIL consortium

Annex M:

Cold Movement Detection And Train Awakening FMEA Report

This document is public

Annex N:

HAZOP for ETCS Applications: Train Integrity

This document is internal to the GRAIL consortium

Annex O:

Train Integrity FMEA Report

This document is public