


Identificação	IT.SIN.064
Designação	Requisitos de Segurança dos sistemas de controlo-comando e sinalização
Versão	01
Data	07.10.2008
Ficheiro	It_sin_064.doc
Classificação	EXT

**Aprovado pelo Sr. Director de Engenharia e Intervenções Especiais**



José Carlos Abrantes dos Santos Clemente

**Aprovado pelo Sr. Director Geral de Engenharia e Construção**



José de Castro Cunha Alves Monteiro

## **Índice:**

	<b>Pág.</b>
<b>Índice</b>	<b>II</b>
<b>Participantes na elaboração do documento normativo</b>	<b>III</b>
<b>Histórico do Documento</b>	<b>III</b>
<b>1. Introdução</b>	<b>1</b>
1.1. Âmbito	1
1.2. Documentos normativos revogados	1
1.3. Abreviaturas, siglas e símbolos	1
1.4. Documentos de referência	1
<b>2. Definição de Requisitos</b>	<b>2</b>
2.1. Enquadramento	2
2.2. Requisitos Gerais	2
2.3. Taxa de Risco	3
<b>3. Metodologia de Análise de Risco</b>	<b>3</b>



IT.SIN.064  
Requisitos de Segurança dos sistemas  
de controlo-comando e sinalização

Versão: 01  
Data: 07.10.2008  
Ficheiro: It\_sin\_064.doc  
Classificação: EXT

**Participantes na elaboração do documento normativo:**

Nome	Empresa	Cargo / Órgão
João Alves	REFER	EN-EIE - Electrotecnia - PERTMS
Luís Brazinha	REFER	EN-EIE - Electrotecnia - PERTMS
Vítor Amaral	REFER	EN-EIE - Electrotecnia - PERTMS

**Histórico do Documento:**

Versão	Descrição	Data
01	Versão Inicial – IT.CCS.007	27.12.2007
01	Renumeração para IT.SIN.064	07.10.2008

## **1. Introdução**

### **1.1. Âmbito**

O presente documento descreve os requisitos de segurança em conformidade com o nível de segurança do sistema para protecção de acidentes.

Este documento visa apresentar os requisitos de segurança (requisitos funcionais de segurança que descrevem como o sistema de encravamento funciona e requisitos de integridade de segurança nos quais é referenciado a taxa de falhas permitida para as funções de segurança) e que caracterizam a taxa de falhas permitida para um sistema de encravamento.

### **1.2. Documentos normativos revogados**

O presente revoga o documento IT.CCS.007 - Requisitos de Segurança dos sistemas de controlo-comando e sinalização de 27.12.2007.

### **1.3. Abreviaturas, siglas e símbolos**

MTBF	tempo médio entre falhas
MTBSiF	tempo médio entre falhas significativas
MTBMaF	tempo médio entre falhas maiores
MTBMiF	tempo médio entre falhas menores
RBC	Centro de Bloco por Rádio
ATP	Sistema Automático de Protecção de Comboios
TCCS	Mesa de Operação do Sistema de Sinalização
THR	Taxa Tolerável de Risco
SIL	Nível de Integridade de Segurança

### **1.4. Documentos de referência**

IT.SIN.066 – Normativos dos sistemas de controlo-comando e sinalização

NP EN 50126:2000 – Aplicações Ferroviárias Especificação e demonstração de Fiabilidade, Disponibilidade, Manutenibilidade e Segurança RAMS

NP EN50129:2005 – Aplicações ferroviárias – Sistemas de sinalização, telecomunicações e de processamento – Sistemas electrónicos de segurança para sinalização

Requisitos de Segurança e Análise de Segurança para Interoperabilidade - Grupo de Utilizadores ERTMS/ETCS

Documento 088 versão 2.2.10 ERTMS/ETCS classe 1 - UNISIG

Documento 091 versão 2.2.11 ERTMS/ETCS classe 1 - UNISIG

Requisitos Qualitativos – Projecto Euro-Interlocking

Requisitos RAM – Grupo de Utilizadores ERTMS/ETCS

## **2. Definição de Requisitos**

### **2.1. Enquadramento**

A Segurança e a Disponibilidade estão relacionadas, podendo em determinadas situações o aumento de Segurança provocar uma diminuição da Disponibilidade e conduzir à realização de operações manuais, devido ao bloqueio do sistema.

Deverão ser definidas primeiramente as fronteiras do Sistema, de modo a serem identificados todos os riscos dentro das fronteiras definidas.

Os riscos podem ser organizados na estrutura de árvores de falhas, constituindo os que se encontram no topo da árvore de falhas, aqueles que poderiam surgir na fronteira do sistema.

### **2.2. Requisitos Gerais**

Após a identificação de cada risco e da função à qual está associado é realizada a análise de consequência, através da identificação das possíveis causas e consequências para cada risco.

Os requisitos funcionais são implementados para assegurar uma função segura.

A eliminação dos riscos tem como objectivo atingir uma taxa de riscos tolerável para as funções correspondentes.

O sistema de encravamento deve possuir funções de segurança que previnam as seguintes situações: colisão entre comboios, descarrilamento de um comboio (ex: em aparelhos de mudança de via), colisão entre comboios e tráfego rodoviário em passagens de nível, colisão de um comboio com equipas de manutenção da infra-estrutura e colisão entre circulações e equipamentos da infra-estrutura.

A função de segurança assume para os respectivos cálculos a existência de 10 entradas e uma saída associada a cada função como ordem de grandeza.

O sistema de encravamento deve ter uma taxa tolerável de risco inferior a  $1 \cdot 10^{-9}$  [1/h] associada a cada função de segurança. Em conformidade com a EN 50129 o requisito atrás indicado deverá corresponder a utilização do nível de integridade de segurança SIL 4.

Os requisitos de segurança são estruturados em requisitos de segurança para o subsistema ETCS instalado no material circulante, na infra-estrutura de via e nos processos de engenharia adoptados no desenvolvimento do Subsistema ETCS.

### 2.3. Taxa de Risco

A abordagem utilizada no subsistema ERTMS/ETCS consiste na atribuição aos diversos constituintes de interoperabilidade da taxa tolerável de risco de forma equitativa:

- THR material circulante =  $1 \cdot 10^{-9}$  [1/h]
  - Elementos integrantes EVC, ODO, MMI, BTM, LTM e funções associadas do material circulante e transmissão;
- THR infra-estrutura =  $1 \cdot 10^{-9}$  [1/h]
  - Elementos integrantes RBC, LEU, eurobaliza, eurolaço e funções associadas do material circulante e transmissão.

A atribuição acima indicada é efectuada com base nos riscos identificados nos constituintes que possam ocorrer numa amostra temporal de uma viagem de uma hora.

As taxas de risco toleráveis estão relacionadas com funções críticas necessárias para assegurar a interoperabilidade técnica, sendo no ponto 3 identificados os eventos que poderão originar um risco que conduzirá a situações inseguras.

O Fornecedor deverá assegurar junto da REFER o controlo de eventos que poderão conduzir a situações inseguras nomeadamente nos seguintes elementos:

- ETCS instalado no material circulante,
- Sistema de transmissão ETCS instalado no material circulante,
- ETCS instalado na infra-estrutura,
- Sistema de transmissão ETCS instalado na infra-estrutura,
- Sistemas adjacentes (Encravamentos e Sistemas de detecção) e Subsistema ETCS que incluem os seguintes processos garante da harmonização do subsistema ETCS (Preparação de Dados, Performance do Sistema, Parâmetros e Dados do Material Circulante adoptados pelo Operador).

Associada à taxa admissível de falhas inferior a  $1 \cdot 10^{-9}$  falhas por hora corresponde o nível de integridade SIL 4, que caracteriza o equipamento ERTMS/ETCS instalado no material circulante e na infra-estrutura.

### **3. Metodologia de Análise de Risco**

A análise de risco efectua a ligação entre a identificação de riscos e os requisitos de segurança.

Uma situação perigosa ocorre quando é registado um desvio dos requisitos funcionais através de uma função, sendo enviado do sistema encravamento ou do subsistema ERTMS/ETCS. Esta função poderia ser o envio incorrecto de um comando de sinal.

Poderá ser assumida a existência limitada de riscos existentes na fronteira do sistema de encravamento e estes poderão integrar uma lista não exaustiva de riscos:

- Envio incorrecto de um comando do sistema de encravamento para um sinal,
- Envio incorrecto de um comando do sistema de encravamento para um sinal, equipamento ATP,
- Envio incorrecto de um comando do sistema de encravamento para um sinal, agulha,
- Envio incorrecto de um comando do sistema de encravamento para um sinal, RBC,
- Envio incorrecto de um comando do sistema de encravamento para um sinal, passagem de nível,
- Envio incorrecto de um comando do sistema de encravamento para um sinal, encravamento adjacente,
- Envio incorrecto de um comando do sistema de encravamento para um sinal, Bloco,
- Envio incorrecto de um comando do sistema de encravamento para um sinal, ERTMS/ETCS equip.infra-estrut,
- Envio incorrecto de um comando do sistema de encravamento para um sinal, TCCS.

A fase seguinte consiste em realizar uma análise de consequência de modo a permitir a identificação de causas e consequências para cada risco.

Os riscos identificados têm associado à sua estimativa um carácter improvável de ocorrerem. Os requisitos funcionais constituintes do sistema são especificados e implementados de forma a terem associado uma função segura.

Em conformidade com a norma EN 50129 é considerada a ocorrência de riscos na fronteira do sistema ETCS.

A identificação de riscos genérica deverá ser complementada pela análise causal que avalia e analisa a implementação da instalação, de forma a identificar novos riscos prováveis de ocorrerem, resultantes da implementação da aplicação específica.

A identificação é efectuada nos documentos referência tendo por base os eventos/riscos verificados na fronteira do sistema e associados aos seguintes modos de falha:

- Função requerida mas não realizada,
- Função realizada mas não requerida,
- Função correcta aplicada ao objecto errado,
- Função incorrecta aplicada ao objecto correcto,
- Falha de Interface,
- Informação errada,
- Informação ausente,
- Informação incompleta,



- Informação incorrectamente ordenada,
- Informação mal endereçada – direcção errada,
- Envio de informação associada dessincronizada – demasiado cedo ou tardio
- Envio de informação associada inconsistente,
- Funcionalidade complexa,
- Falta de comunicação,
- Informação negligente,
- Informação sem referencial de data.

A análise de risco a apresentar pelo Fornecedor do Subsistema ETCS deverá contemplar para cada função associada, os seguintes campos:

- Modo de falha,
- Descrição e explicação da função associada,
- Indicação de limitações – campos não abrangidos pela função,
- Análise simplificada da consequência – possíveis consequências directas do risco,
- Exemplo das causas para a ocorrência do risco, anotações – referências a acções/conteúdos importantes não mencionados,
- Verificação da fronteira do sistema – alocação do risco de acordo com a estrutura do sistema.

O processo de análise de risco realizado pelo Fornecedor deverá ser fundamentado nas metodologias aplicadas e pressupostos assumidos, devendo acompanhar o relatório de conformidade dos requisitos de segurança as aplicações e metodologias empregues.

Constitui elemento integrante do relatório acima referido a aplicação e demonstração do processo de análise de risco, podendo referenciar o nível de integridade de segurança requerido às diversas funções do sistema.