



Rete Ferroviaria Italiana  
10/12/2002

RFI-DTC\  
A0010\PI\2002\0000554

Direzione Tecnica  
il Direttore

MINISTERO DELLE INFRASTRUTTURE E DEI  
TRASPORTI

Dipartimento per i trasporti terrestri e per i sistemi  
informativi e statistici

Direzione Generale del Trasporto Ferroviario  
Via Caraci, 36 00157 Roma

TRENITALIA S.p.A.

Sig. Direttore

Unità Tecnologie Materiale Rotabile

Via Spartaco Lavagnini, 58 50129 FIRENZE

Italferr S.p.A.

Sig. Presidente e Amministratore Delegato

Via Marsala, 53 ROMA

RETE FERROVIARIA ITALIANA S.p.A.

Sig. Amministratore Delegato SEDE

RETE FERROVIARIA ITALIANA S.p.A.

(vedi elenco annesso)

Oggetto: Disposizione N° 32 del 12 Novembre 2002

Allegato 1

Si trasmette copia della Disposizione N° 32, emessa in data 12 Novembre 2002 a firma del Sig. Direttore della Direzione Tecnica, che disciplina la "**Applicazione della normativa CENELEC di settore allo sviluppo e realizzazione di sistemi e prodotti elettronici in sicurezza per il segnalamento ferroviario**"

Si invitano le Strutture in indirizzo a voler confermare il ricevimento della presente restituendo l'allegato modello prestampato.

Michele Elia

Piazza della Croce Rossa, 1 - 00161 Roma

Rete Ferroviaria Italiana Società per Azioni - Gruppo Ferrovie dello Stato

Sede legale: Piazza della Croce Rossa, 1 - 00161 Roma

Cap. Soc. Euro 20.358.109.952

Iscritta al Registro delle Imprese di Roma

Cod. Fisc. n. 01585570581

Direzione Tecnica  
Il Direttore

DISPOSIZIONE N° 32 /2002 del 12 NOV. 2002

**“Applicazione della normativa CENELEC di settore allo sviluppo e realizzazione di sistemi e prodotti elettronici in sicurezza per il segnalamento ferroviario”**

### Il Gestore dell’Infrastruttura Ferroviaria Nazionale

Visto il D.P.R. 11 luglio 1980, n. 753, recante “Nuove norme in materia di polizia, sicurezza e regolarità dell’esercizio delle ferrovie e altri sistemi di trasporto”;

Vista la legge 17 maggio 1985, n. 210, recante “Istituzione dell’Ente Ferrovie dello Stato”;

Visto il D.L. 11 luglio 1992, n.333 - convertito nella legge 8 agosto 1992, n. 359 - recante “Misure urgenti per il risanamento della finanza pubblica”;

Visto il D.P.R. 8 luglio 1998, n. 277, concernente “Regolamento recante norme di attuazione della direttiva 91/440/CEE, relativa allo sviluppo delle ferrovie comunitarie”;

Visto il D.P.R. 16 marzo 1999, n. 146, concernente “Regolamento recante norme di attuazione della direttiva 95/18/CE, relativa alle licenze delle imprese ferroviarie, e della direttiva 95/19/CE, relativa alla ripartizione delle capacità di infrastruttura ferroviaria e alla riscossione dei diritti per l’utilizzo dell’infrastruttura”;

Visto l’art. 131 della legge 23 dicembre 2000, n. 388, recante “Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (Legge Finanziaria 2001)”;

Visto il Decreto del Ministero dei Trasporti del 31 ottobre 2000, n. 138-T, concernente il rilascio alle “Ferrovie dello Stato - Società di Trasporti e Servizi per Azioni” della concessione per la gestione dell’infrastruttura ferroviaria nazionale.

Visti i regolamenti emanati ai sensi dell’articolo 95 del D.P.R 11 luglio 1980, n. 753 sopra citato;

La presente disposizione è composta di n° 7 (sette) pagine

Piazza della Croce Rossa, 1 - 00161 Roma

E' COPIA CONFORME ALL'ORIGINALE  
COMPOSTA DI N°7 (sette) PAGINE

Rete Ferroviaria Italiana Società per Azioni - Gruppo Ferrovie dello Stato  
Sede legale - Piazza della Croce Rossa, 1 - 00161 Roma  
Cap. Soc. Euro 20.538.109.952  
Iscritta al Registro delle Imprese di Roma  
Cod. Fisc. n. 01585570581





Visto l'articolo 8, comma 1, del D.P.R. 11 luglio 1980, n. 753 sopra citato;

Visto il punto 4.2.j), del Decreto Dirigenziale 22 maggio 2000, n. 247/VIG3, emanato dal Servizio di Vigilanza sulle Ferrovie del Ministero dei Trasporti e della Navigazione, avente per oggetto la definizione degli standard e delle norme di sicurezza applicabili al trasporto ferroviario ai sensi dell'articolo 5, comma 1 del D.P.R. 8 luglio 1998, n. 277 (quest'ultimo modificato dall'art. 7 comma 1 del D.P.R. 16 marzo 1999, n. 146);

Visto l'Ordine di Servizio Organizzativo del 7 maggio 2001, n. 424/AD, dell'Amministratore Delegato delle Ferrovie dello Stato S.p.A. che attribuisce al Responsabile della Direzione Tecnica della Divisione Infrastruttura il compito di emanare disposizioni - istruzioni e prescrizioni in materia di sicurezza della circolazione dei treni e dell'esercizio ferroviario;

Vista la Comunicazione Organizzativa del 16 luglio 2001, n. 1/AD, dell'Amministratore Delegato della Rete Ferroviaria Italiana S.p.A. che conferma per RFI le missioni, l'organizzazione, le responsabilità e le procedure già in atto presso la Divisione Infrastruttura ai sensi dell'O.S.O. indicato all'alinea precedente;

Vista la disposizione n° 29, in data 15.10.2002, dell'Amministratore Delegato di Rete Ferroviaria Italiana S.p.A., con cui si dispone che lo sviluppo e la realizzazione di sistemi e prodotti tecnologici per la sicurezza della circolazione ferroviaria siano effettuati nel rispetto della normativa CENELEC pertinente, sulla base di disposizioni emanate dal responsabile della Direzione Tecnica ai sensi e per gli effetti di cui agli articoli 95-99 d.p.r. 753 / 1980 e 7 ed 11 d.lgs. 146/1999 e secondo le procedure dettate dalla Direzione stessa;

Vista la relazione del Responsabile della S.O. Sicurezza e Segnalamento del 18.10.2002 protocollo RFI/TC.SS/009/421, che propone l'emanazione, ai sensi e per gli effetti di cui agli articoli 95-99 d.p.r. 753 / 1980 e 7 ed 11 d.lgs. 146/1999, di una disposizione che disciplini i processi, i criteri per l'effettuazione dell'analisi del rischio e gli aspetti di sicurezza tecnologica relativamente allo sviluppo e realizzazione di sistemi e prodotti elettronici in sicurezza per il segnalamento ferroviario;

Ritenuta la necessità e l'opportunità di emanare la presente disposizione

## DELIBERA

### ARTICOLO 1 GENERALITÀ

- 1.1 La presente disposizione pone i principi per l'applicazione della normativa CENELEC di settore allo sviluppo e realizzazione di prodotti e sistemi





elettronici in sicurezza per il segnalamento ferroviario, di terra e di bordo, relativi all'infrastruttura ferroviaria nazionale.

- 1.2 A decorrere dalla data di emissione della presente disposizione lo sviluppo e realizzazione di prodotti e sistemi elettronici in sicurezza per il segnalamento ferroviario dovrà essere effettuato in base alla normativa CENELEC di settore con le specificazioni sancite nella presente disposizione.
- 1.3 Le attività di sviluppo o realizzazione di prodotti e sistemi che alla data di emissione della presente disposizione sono già state avviate possono di regola essere completate applicando le norme e le procedure iniziali. La Direzione Tecnica di RFI, può comunque richiedere l'applicazione della presente disposizione o di ben identificate parti di essa in relazione allo stato di avanzamento delle attività in corso.
- 1.4 I prodotti e sistemi che alla data di emissione della presente disposizione, sono già corredati di "*Certificato di Omologazione*" rilasciato dalle competenti S.O. di RFI, in accordo con le procedure precedentemente vigenti, devono ritenersi utilizzabili a tutti gli effetti, se è rispettato il previsto contesto applicativo. L'utilizzo di tali prodotti e sistemi, all'interno di sistemi più complessi, sviluppati in accordo alla normativa CENELEC, è da ritenersi accettabile. In questo caso non si rende necessaria l'adozione di alcuna procedura integrativa.

## ARTICOLO 2 DEFINIZIONE DEI PROCESSI

- 2.1 Devono essere considerati due processi di riferimento: processo di sviluppo e processo di realizzazione. In entrambi i processi la normativa CENELEC di settore deve essere applicata per tutte le fasi del ciclo di vita del Prodotto o Applicazione Generica o Applicazione Specifica.
- 2.2 Il processo di *sviluppo* riguarda la omologazione di un Prodotto Generico o di una Applicazione Generica.





- 2.3 Il processo di *realizzazione* riguarda l'attivazione all'esercizio di una Applicazione Specifica ricavata, di norma, da una Applicazione Generica omologata.
- 2.4 La *valutazione* è una macrofase del processo di sviluppo di un prodotto o sistema. Risulta dalla integrazione di:
- *Valutazione funzionale* (Functional Assessment),
  - *Valutazione di sicurezza* (Safety Assessment)
- La *valutazione* riguarda i documenti di progetto e di verifica e validazione prodotti dal Fornitore che ha piena e completa responsabilità penale e civile di quanto in essi contenuto.
- 2.5 La responsabilità della *valutazione, della valutazione funzionale e di quella di sicurezza*, viene assegnata alle S.O. specialistiche secondo le attribuzioni specifiche definite negli ordini di servizio organizzativi; dette S.O. potranno avvalersi, per l'espletamento delle relative attività, di enti terzi, indipendenti dal Fornitore, qualificati o notificati che assumono piena responsabilità penale e civile per le specifiche attività svolte.
- 2.6 La qualificazione e la notificazione, la sorveglianza e l'Audit degli Enti terzi e dei Fornitori saranno disciplinate da apposite procedure.
- 2.7 È ammesso non ripetere le attività di *Valutazione di sicurezza* (Safety Assessment) nel caso in cui sia disponibile la documentazione di conformità alle Norme CENELEC di riferimento rilasciata dalle Autorità di sicurezza (Safety Authority) di altre nazioni o da organismi notificati.

### ARTICOLO 3 CRITERI PER L'EFFETTUAZIONE DELL'ANALISI DEL RISCHIO

- 3.1 L'analisi del rischio deve essere condotta a livello di sistema con le modalità definite nei punti successivi. Tale attività non viene in genere richiesta per modifiche di natura puramente tecnica.





- 3.2 L'analisi del rischio nell'esercizio ferroviario deve essere condotta in modo da consentire la tracciabilità delle valutazioni (qualitative) fatte per dimostrare che per ogni pericolo (hazard) individuato sono state definite "le misure e le cautele suggerite dalla tecnica e dalla pratica, atte ad evitare sinistri", come prescritto nell'articolo 8, comma 1, del DPR 753 dell'11 Luglio 1980. L'adozione delle misure e delle cautele così definite per ciascuno dei pericoli individuati consente di "minimizzare il rischio di incorrere in eventi incidentali", conformemente a quanto disposto nel Decreto Dirigenziale 247/VIG3 del 22/5/2000 comma 4.2.j.
- 3.3 La minimizzazione del rischio si consegue adottando quanto suggerito dalla tecnica e dalla pratica per il contesto applicativo di riferimento, e deve consentire di ottenere un livello di rischio residuo *trascurabile*, attribuendo a questo termine la definizione data nella norma EN 50126.
- 3.4 Si ritiene accettabile un rischio minimizzato attraverso l'adozione di misure e cautele corrispondenti al massimo dello stato dell'arte, ossia al livello ultimo della tecnica e della pratica raggiungibile, in modo conveniente, in un determinato momento per il settore considerato.
- 3.5 Misure basate su parametri quantitativi potranno essere utilizzate solo quando ciò sia espressamente previsto a livello legislativo nazionale oppure a livello di normazione tecnica comunitaria con espressa indicazione delle metodologie di valutazione.
- 3.6 Di norma, i prodotti e i sistemi che contengono funzioni correlate alla sicurezza della circolazione ferroviaria devono avere il livello di integrità della sicurezza (SIL: Safety Integrity Level, definito nella norma CENELEC EN50129) pari a 4. È comunque ammesso che le sottoparti con funzioni di sicurezza, di tali prodotti e sistemi possano avere SIL inferiore, con un livello minimo di SIL pari a 2, solo nel caso in cui ci sia adeguata copertura procedurale che consenta comunque il raggiungimento, a livello di sistema, di un SIL pari a 4.
- 3.7 È ammesso effettuare analisi di rischio di tipo comparativo, per funzioni già presenti (o simili a quelle presenti) nello scenario ferroviario, accettando per esse soluzioni tecnologiche specifiche allineate al corrente stato dell'arte.





- 3.8 Possono essere utilizzati, durante la fase di realizzazione di una Applicazione Specifica, prodotti o strumenti che possono avere anche un SIL pari a 0 (ad esempio commerciali) purché siano utilizzati al di fuori dell'ambito operativo ed a condizione che la procedura definita per il loro utilizzo permetta di dare evidenza del raggiungimento del SIL richiesto..
- 3.9 Non è obbligatorio condurre l'analisi del rischio né per le Applicazioni Specifiche correlate ad una Applicazione Generica omologata né per nuove Applicazioni Generiche se entrambe caratterizzate dal corretto e completo rispetto dello stesso contesto di riferimento, funzionale e normativo definito nella precedente omologazione della Applicazione Generica.

#### ARTICOLO 4 SICUREZZA DEI PRODOTTI E DEI SISTEMI TECNOLOGICI

- 4.1 Per un prodotto o sistema il cui utilizzo è correlato alla sicurezza della circolazione, il Fornitore deve dare piena evidenza della sua sicurezza tecnica dimostrando nel dettaglio che si sono adottate soluzioni adeguate a soddisfare i requisiti associati al SIL definito in fase di analisi del rischio per ciascun pericolo identificato.
- 4.2 Di norma, l'analisi dei pericoli (hazard analysis) deve essere condotta dimostrando che per ogni pericolo si sono introdotte, sul piano tecnico ed a livello del singolo sottosistema o elemento considerato, contromisure adeguate che consentono di ritenere che il pericolo stesso sia adeguatamente controllato. Le valutazioni numeriche, che comunque devono rispondere a quanto prescritto dalle norme CENELEC, sono da considerare come elementi di integrazione del processo di valutazione della sicurezza.
- 4.3 La documentazione di conformità di un prodotto o sistema in uso alle norme CENELEC di settore, rilasciata dall'Autorità di sicurezza di altre nazioni o da organismi notificati, se disponibile e se adeguata al contesto applicativo, corredata dal *rapporto di valutazione* (Assessment Report) e dal *dossier di sicurezza* (Safety Case), è da considerare a tutti gli effetti prova di piena evidenza tecnica della sicurezza del prodotto o sistema considerato e non richiede ulteriori valutazioni dell'adeguatezza delle soluzioni tecniche adottate ai fini della sicurezza.





- 4.4 Per prodotti e sistemi che non rientrano nella casistica definita al precedente punto 4.3, sono ritenute soluzioni tecnicamente adeguate tutte quelle realizzate nel rispetto delle norme CENELEC a livello di procedure, documentazione e provvedimenti tecnici, in relazione al SIL da considerare, e non in contrasto con le indicazioni dei successivi punti 4.4.1 e 4.4.2.
- 4.4.1 Non sono considerate di norma accettabili le soluzioni che prevedano la rivelazione del guasto tramite intervento manutentivo e/o che richiedano oneri aggiuntivi di qualsiasi tipo per la gestione del prodotto o sistema.
- 4.4.2 Per prodotti o sistemi per i quali è richiesto un SIL pari a 4, la rilevazione e negazione del guasto deve essere effettuata dal sistema attraverso adeguati cicli di test ed il relativo *“tempo di rilevazione e negazione del guasto”*, di norma definito a livello di capitolati tecnici generali o di specifica dei requisiti, deve essere comunque inferiore, per ciascuna delle funzioni di sicurezza del prodotto o del sistema sviluppato, al tempo minimo richiesto per la sua attuazione (Annex B.3.3 della Norma EN 50129).
- 4.5 Soluzioni tecniche non rispondenti ai punti 4.4.1 e 4.4.2, saranno considerate accettabili o se espressamente previste negli allegati tecnici ai documenti contrattuali di RFI o se il Fornitore dimostra alla Direzione Tecnica di Rete Ferroviaria Italiana, attraverso una idonea e particolareggiata documentazione, che esse risultano vantaggiose in termini di miglioramento degli aspetti prestazionali e/o operazionali e/o manutentivi, della riduzione dell'impatto sulla normativa e della maggiore tempestività e/o flessibilità realizzativa.
- 4.6 Per l'applicazione di prodotti o sistemi sviluppati non in ambito RFI prima dell'emanazione della normativa CENELEC è richiesta documentazione analoga a quella di cui al punto 4.3 o la dimostrazione di largo impiego degli stessi presso primarie reti ferroviarie, con evidenza che le soluzioni tecnologiche adottate possono essere riconosciute comunque come *“stato dell'arte”* per il contesto applicativo da considerare. In tali casi i prodotti o sistemi saranno considerati accettabili se la Direzione Tecnica di RFI, sulla base di una dettagliata documentazione dimostrativa, ne autorizza l'applicazione.

Michele Mario Elia

