CERTIFER

Bureau d'Enquêtes sur les Accidents de Transport Terrestre
Monsieur Jean-Damien PONCET
Directeur
Grande Arche - Paroi Sud
92055 LA DEFENSE Cedex

Valenciennes, le 28 octobre 2021

Nos Réf. : DT/PO/SM/0013

Objet : Votre correspondance du 29/07/2021

Monsieur le Directeur,

Nous avons lu attentivement le rapport d'enquête technique sur la survitesse d'un TGV à La Milesse (72) le 22 décembre 2019.

Ce rapport formule une recommandation R4 adressée à CERTIFER que nous rappelons :
« Revisiter la méthodologie de l'évaluation concernant la « validation du système » selon les normes CENELEC 50126 et suivantes afin de garantir la validité de l'évaluation ».

La lecture détaillée du rapport indique que cette recommandation porte sur la validation des paramètres qui sont utilisés par les calculateurs ERTMS (plus exactement le RBC).

Afin de prendre en compte cette recommandation R4, CERTIFER a rédigé une RFU relative à « l'évaluation du processus de paramétrage » que vous trouverez en pièce jointe.

Les RFU de CERTIFER sont des documents internes CERTIFER, applicables (sauf justification étayée), qui précisent ou clarifient des exigences règlementaires ou des exigences issues de normes. Cette RFU sera référencée par notre référentiel RF0015 « Pour la Certification du niveau d'intégrité de la sécurité des produits ou systèmes selon les normes CENELEC EN50126, EN50128, EN50129 », l'application de ce référentiel RF0015 étant contrôlé par le COFRAC lors de ces audits périodiques de CERTIFER.

Nous proposons également l'échéancier suivant pour la mise en œuvre de cette action :
- 1 mois après l'accord du BEATT sur notre proposition d'action : officialisation de la RFU « évaluation du processus de paramétrage » et information du personnel sur la RFU a appliquer
- 6 mois après l'accord du BEATT, mise à jour du référentiel RF0015 pour ajouter une référence à la RFU « évaluation du processus de paramétrage »

CERTIFER SA - Siège social : 18, rue Edmond Membrée - CS 40141 - F 59308 Valenciennes Cedex
Tél. : +33 (0)3 27 28 35 00 - Fax : +33 (0)3 27 28 35 09 - www.certifer.eu
Société Anonyme au capital de 9.000.180€ - TVA/SIRET : FR28 802 053 397 00039 - NAF : 7120B - RCS Valenciennes 802 053 397

La RFU « évaluation du processus de paramétrage », encore en version projet, est en annexe 1.

Nous nous tenons à votre disposition pour échanger sur les propositions faites.

Veuillez agréer, Monsieur le Directeur, l'expression de mes sentiments les meilleurs.

Pierre KADZIOLA
Directeur Général

CERTIFER
18, rue Edmond Membrée
59300 Valenciennes
FRANCE

TITLE	
EVALUATION DU PROCESSUS DE PARAMETRAGE	
ORIGINATOR	**SUBJECT RELATED TO**
CERTIFER SA	Processus de paramétrage

AMENDMENT RECORD:

Issue 01: Creation

Issue 02:

Issue 03:

DESCRIPTION AND BACKGROUND EXPLANATION

Le 22 décembre 2019 une survitesse d'un Train Grande Vitesse s'est produite sur la Ligne à grande Vitesse Bretagne Pays de Loire, alors que ce TGV circulait en ERTMS Niveau 2.

Le rapport d'enquête technique réalisé par le BEATT conclut que cette survitesse (165 km/h au lieu de 100 km/h sur une aiguille en voie déviée) est due à une erreur de paramétrage du RBC.

Dans son analyse, le rapport d'enquête indique (§3.6.4 Analyse et conclusion ») :

« *Afin de justifier la sécurité d'un système, les règles de « méthode de sécurité commune » posent pour l'intégration des sous-composants spécifiés et construits pour le système que « dans le cas des sous-systèmes développés selon un code de bonne pratique, cela inclut les preuves de conformité de la réalisation conformément au code de bonne pratique utilisé ». Ces dispositions figurent aujourd'hui dans la nouvelle norme EN50126-1 version 2017.*

Or au titre de ces « bonnes pratiques » dans le cadre d'une mise en œuvre rigoureuse du cycle en V, le paramétrage doit faire l'objet d'une vérification, doublée d'une validation. Les contrôles techniques de validation sont à faire de façon exhaustive, sur la base des documents d'exécution de même niveau, c'est-à-dire les documents qui ont posé le besoin. Dans notre cas, ce sont les plans techniques. Ici, les essais sur plateforme ont omis la validation du paramétrage des profils de vitesse, laissant perdurer les erreurs de vérification préalablement commises. Enfin, la dernière vérification du paramétrage effectuée (3ième vérification) l'a été sur la base de données du fichier COTAGE qui sont d'un niveau inférieur à celui des plans techniques qui ont posé le besoin. Elle ne constituait ainsi pas une validation. »

Le rapport d'enquête indique également (§5.5 L'évaluation de la sureté de fonctionnement) :

« *La règle lors d'une utilisation rigoureuse du cycle en V, fixe que les vérifications sont doublées de validations effectuées sur la base du besoin exprimé sur le niveau*

d'intégration sur lequel on se situe. Cette règle est appelée dans les normes CENELEC 50126 et suivantes en tant que « bonne pratique ».

Les profils de vitesse de la traversée 7201-7202 n'ont pas fait l'objet d'une validation sur la base du besoin exprimé, à savoir le plan technique qui décrit de manière détaillée la constitution de la signalisation. La stratégie d'essai en plateforme retenue ne couvrait pas le contrôle des profils de vitesse. L'évaluateur CERTIFER n'a pas relevé cet écart avec cette exigence de validation selon les normes CENELEC. »

Le rapport d'enquête formule la recommandation suivante :

« Recommandation adressée à CERTIFER : revisiter la méthodologie de l'évaluation concernant la « validation du système » selon les normes CENELEC 50126 et suivantes afin de garantir la validité de l'évaluation ».

RFU

- Concernant la planification de l'évaluation, le Plan d'Evaluation devra prévoir, pour les fonctions SIL4, un audit technique relative au processus de paramétrage et son implémentation

- Concernant l'évaluation des processus de paramétrage, les évaluateurs devront considérer les exigences suivantes des normes CENELEC afin de formuler leur avis :

  a) EN50128 version 2011/A2 2020 §8 Développement de données d'application ou d'algorithmes d'application : systèmes configurés par des données d'application ou par des algorithmes d'application.

  b) EN50128 version 2011 Table A1 Documentation. CERTIFER devra évaluer la documentation relative à l'application du processus de paramétrage, et que celle – sont conforme à la documentation prévue dans la Table A.1

  c) EN50128 version 2011 table A11 techniques de préparation des données : CERTIFER devra évaluer les techniques mises en œuvre, et s'assurer que les exigences considérées « M » (Mandatory en anglais, Obligatoire en Français) par la norme sont largement utilisées : tests fonctionnels et Checklists.

- L'utilisation d'outils de vérification, de tests, voire d'outils de preuves formelles sera fortement encouragée par les évaluateurs. Les outils utilisés devront être conformes aux exigences de EN50128 §6.7 Outils et Langage

- De plus l'évaluateur devra s'assurer que:

d) les tests permettent de couvrir de façon exhaustive l'ensemble des paramètres, sur la base de documents qui ont posé le besoin. (cela peut se faire par exemple sur la base d'un rapport de vérification préparé par le demandeur). (voir également EN50128 D.2)

e) les « chargés de vérifications » réalisant des activités de vérification manuelles devront être compétents (cela peut se faire par exemple sur la base des formations et des expériences professionnelles délivrés par le demandeur). En cas de double vérification manuelle, les activités de vérifications devront se faire dans des conditions préservant l'indépendance des « chargés de vérifications ». (voir aussi EN50128 §5.2 compétence du personnel)

f) en cas d'itération des activités de vérifications manuelles, par exemple suite à des modifications du paramétrage, le demandeur justifie les activités de non régression (analyse d'impact des modifications apportées). (voir aussi EN50128 §9.2.4.8 et §9.2.4.10)

MEMBERS OF THE WORKSHOP

CARLIER Jerome
GROSSIN Olivier
LAFORME Annette
OZELLO Patrick

APPENDIX 1 : PROCEDURE 85 DEFINITION OF DEVIATIONS

Statut	Signification
Ouvert	CERTIFER est en attente d'une réponse ou d'un complément de réponse.
Clos	CERTIFER accepte la réponse : point fermé.
Clos sous réserve de modification documentaire (Clos_SRMD)	Le point est clos sur la base des réponses apportées, mais CERTIFER attend une modification de la documentation lors de la prochaine évolution du document (non urgent, cette modification peut intervenir après la remise du rapport d'évaluation CERTIFER).
Observation	Il peut s'agir de la description d'un sujet, d'un constat neutre ou de tout autre sujet qui mérite d'être mentionné.
Non-conformité mineure (minor_NC)	Toute non-conformité individuelle n'altérant pas l'opérabilité du système de management, du produit ou du système, et non mentionnée comme majeure, telle que :

Le terme « Remarque » peut également être utilisé	- une documentation incomplète ou une mise en œuvre incomplète d'une exigence applicable du règlement, de la norme ou des exigences du client, à condition que la documentation manquante ne soit pas essentielle pour l'opération ; - le manque de preuves pour démontrer la conformité avec une exigence applicable de la réglementation, de la norme ou des exigences du client, si cela n'altère pas la confiance dans la mise en œuvre d'un élément essentiel du système de gestion de la qualité ou de la sécurité, du produit ou du système. Les non-conformités mineures sont mentionnées dans le rapport d'évaluation.
Non-conformité Majeure (major_NC)	- Le système de management ne garantit pas la conformité des activités de maintenance et d'exploitation avec les exigences de la réglementation applicable et/ou du système de gestion de la qualité mis en œuvre ; - une planification insuffisante du système de management compte tenu des objectifs à atteindre ; - plan de gestion insuffisant, inadapté ou inexistant ; ou manque de ressources pour satisfaire aux exigences de la règlementation et/ou d'une exigence du système de gestion de la qualité ; - absence d'une composante essentielle du système de management : aucune preuve de la documentation ou de la mise en œuvre d'une exigence (ou d'une partie significative d'une exigence) du règlement et/ou d'une exigence du système de gestion de la qualité ; - dans le cas où seule une partie d'une composante du système de management est manquante, mais que cette partie manquante a une influence critique sur le fonctionnement global du système et sur les produits ou services fournis maintenance et/ou les produits ou services fournis et ce, dans la mesure où les conséquences négatives de cette défaillance sont identifiées dans la période passée; - une non-conformité manifeste ou délibérée par rapport à une exigence légale ou réglementaire et/ou d'une exigence du système de gestion de la qualité ou de la sécurité ; - une accumulation de non-conformités mineures qui conduit à un manque de confiance dans l'efficacité du système ; - un délai trop long pour la résolution des demandes d'actions correctives établies par l'équipe d'audit, de telle sorte que la capacité de l'organisme à les traiter peut être mise en doute ; - lorsqu'une non-conformité est telle que l'équilibre du système de management de la qualité et de la sécurité et son fonctionnement global sont faussés. - situation conduisant à un danger direct pour la sécurité de l'exploitation ferroviaire ; - la violation d'une exigence légale, réglementaire, normative ou d'un client qui met en cause la sécurité de l'exploitation; - violation d'une loi, d'un règlement, d'une norme ou d'exigences du client qui remet en cause l'utilisation opérationnelle du produit ou du système ; Les non-conformités majeures sont mentionnées dans le rapport d'évaluation et doivent être corrigées dans un délai donné afin d'obtenir ou de conserver le certificat.
Ecart technique	La réponse confirme un écart par rapport à une exigence de référence. La criticité de l'écart dépend des conditions d'utilisation du système ou du produit, alors il n'est pas possible pour l'évaluateur d'estimer la criticité. Les écarts techniques peuvent être liés à des caractéristiques techniques (fonctions, interfaces, performances). Les écarts techniques sont mentionnés dans le rapport d'évaluation.
Sujet à réévaluer	Des activités obligatoires prévues par les documents de référence qui ne sont pas finalisées, peuvent être qualifiées de "non-conformités". ou explicitement décrites comme "sujettes à réévaluation lors d'une prochaine phase" dans la conclusion.

lors d'une prochaine phase	