



MADE IN
FRANCE

CLEARSY DATA SOLVER

CLEARSY DATA SOLVER



clearsy
Safety Solutions Designer

VALIDATION FORMELLE DE DONNEES
CLEARSY DATA SOLVER

CONTACT@CLEARSY.COM

CLEARSY DATA SOLVER

Dans le ferroviaire, les logiciels critiques pour la sécurité sont développés et validés indépendamment des données qui les paramètrent. Par exemple, la topologie de la voie, les positions des signaux et des aiguilles, les points kilométriques, sont des données constantes utilisées par un pilote automatique pour calculer les courbes de freinage et déterminer à quel moment déclencher le frein d'urgence.

Ainsi, chaque partie doit être sûre au même niveau selon l'EN 50128 : SIL4.

Le processus de validation des données consiste à s'assurer que l'ensemble des données sont correctes. Par exemple : dans la norme ferroviaire ERTMS, les voies sont équipées avec des signaux et des balises. Des règles à vérifier sont relatives à la topologie : chaque signal (feu) doit avoir un groupe de balises associé, la distance entre la première balise et le feu, ou entre deux balises doit être inférieure à deux mètres. D'autres règles concernant le paramétrage sont vérifiées : le contenu des messages envoyés par les balises au train (distances, gradients, vitesses, etc.).

Auparavant, le processus de validation manuelle des données était entièrement humain, menant à des activités à longues et importantes, sujettes aux erreurs (demandant plusieurs mois pour vérifier manuellement jusqu'à 1000 règles sur plus de 100 000 données). La validation formelle des données est l'évolution naturelle de ce processus humain en un processus automatique et sécurisé. CLEARSY a inventé cette approche grâce à ses connaissances et compétences approfondies sur la technologie des méthodes formelles et les outils associés.



Aperçu de l'outil CLEARSY Data Solver

CLEARSY fournit un outil de validation de données et ses services associés. **Les bénéfices de cette approche formelle sont variés :**

- **Rapidité** : seules quelques heures suffisent pour valider un projet ferroviaire complet.
- **Automatique, exhaustif**, presse bouton et répétable à l'envie (évite les activités de non régression fastidieuse).
- **Supprime les erreurs humaines**, par l'utilisation d'une méthode formelle (donc d'un formalisme non ambigu) et de techniques certifiées.
- Permet **une forte réutilisation** des règles d'un projet à l'autre (capitalisation des connaissances).
- La solution est basée sur **un outil certifié T2**.
- Vise principalement les projets ferroviaires types : CBTC, ERTMS, RBC, ATS...

Pourquoi cette approche est meilleure que l'utilisation de scripts ou d'algorithmes écrits en C++/Python ?

- Les scripts sont utilisés pour faire des petites vérifications mais ne sont pas efficaces dès qu'il y a de la **complexité**... Et les règles de vérification des CBTC sont très complexes.
- Les scripts et les algorithmes sont difficilement **maintenables** car ils reposent sur des choix d'architecture ou de modélisation. Donc un simple changement dans la spécification peut les rendre obsolètes.
- La grande force du langage B est son **expressivité** : moins de code à produire pour exprimer les propriétés désirées et code plus proche de la spécification.
- La seule partie produite dans les règles formelles est la sélection des données et les propriétés à respecter. Tout le reste est **automatiquement généré** par le Data Solver.
- Une plus grande **robustesse** : ProB et le Data Solver sont utilisés dans des projets industriels par les grands acteurs du ferroviaire, et bénéficie donc d'un grand retour d'expérience.
- Dans la validation formelle de données, les règles sont **indépendantes entre elles**, mais également **indépendantes des données** qu'elles valident. Contrairement aux scripts ou algorithmes, un changement dans le format des données n'affecte donc pas les règles formelles.

DESCRIPTION DU PRODUIT

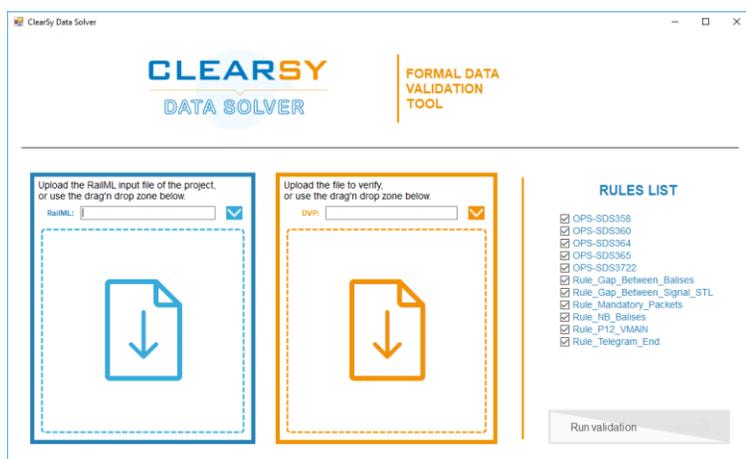
Un outil sur mesure

- Adapté aux formats de données des clients (xml, xls, parameter file, railML, csv, txt ...).
- Format des rapports de vérification adapté au processus client.
- Le client final peut également spécifier ses propres règles et utiliser l'outil.

Un service de développement des règles de vérification formelle

L'outil est un solver qui va vérifier les données concernées règle par règle. Ces règles peuvent être développées par le client ou par CLEARSY. Le service proposé est le suivant :

- Modélisation du modèle formel contenant les règles que les données doivent respecter.
- Ces modèles sont facilement lisibles après une formation.
- Les règles appartiennent ensuite au client qui peut donc les réutiliser autant que souhaité sur les différentes itérations d'un projet ou sur d'autres projets.

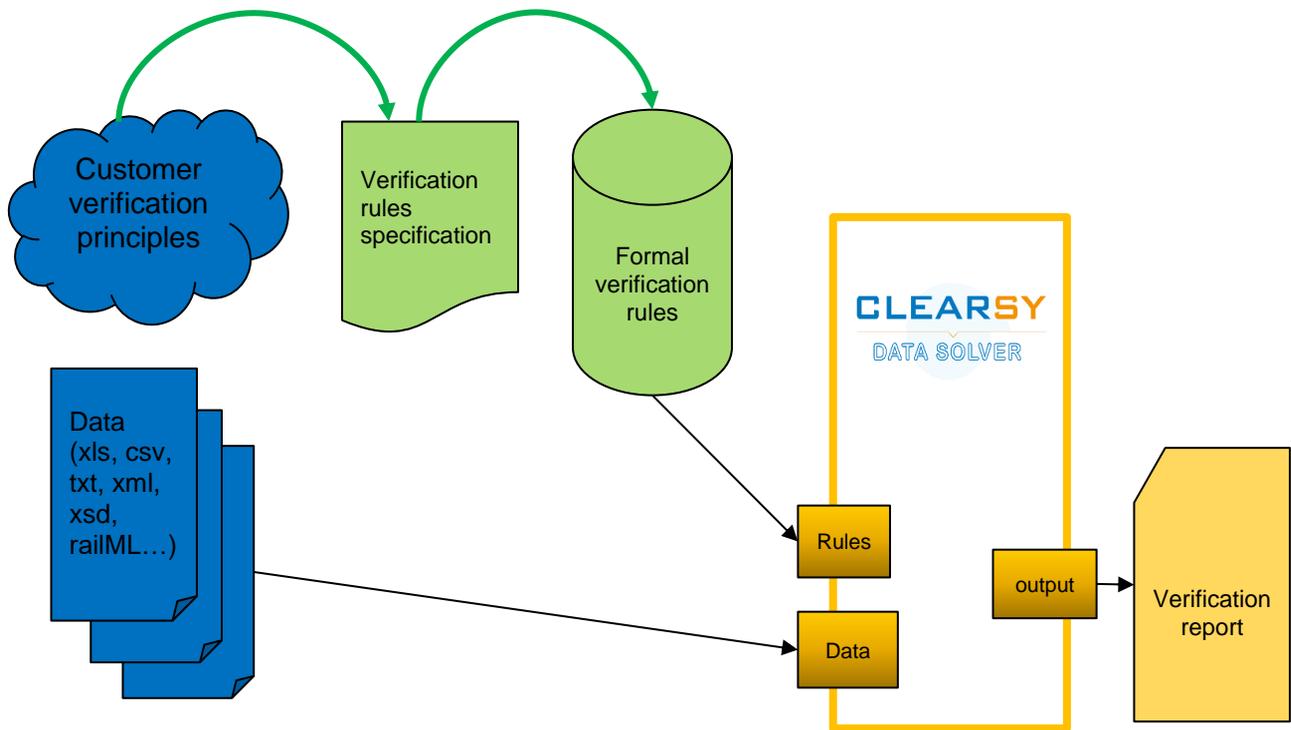


Interface de l'outil de validation formelle de données



L'outil est certifié T2 selon la norme CENELEC EN 50128

PRINCIPES



Les contre-exemples sont écrits en langage naturel et donc compréhensibles par les équipes s'occupant de la génération ou la validation des données.

La liste des contre-exemples est exhaustive, et si aucune erreur n'est reportée les données sont donc validées.

Les rapports contiennent toutes les informations relatives aux campagnes de vérification. Ils peuvent également inclure **la traçabilité des données vérifiées**, les éventuels trous de vérification, les signatures des fichiers d'entrées, etc.

REFERENCES COMMERCIALES

Les clients sont les grand industriels ou les donneurs d'ordre du marché ferroviaire.



Pour ALSTOM (CBTC)



- Depuis 2012
- Outil spécifique développé par CLEARSY
- Plus de 15 projets CBTC vérifiés
- Développement de plus de 2000 règles
- Formation des équipes client

Pour GE transportation (CBTC + IXL)



- 2014-2016
- Nouvel outil développé par CLEARSY, améliorations des performances
- 1000 règles développées en 18 mois
- Couverture des données vérifiées

Pour ATOS et SNCF : paramétrage du système MISTRAL NG (futur système de commande/contrôle centralisé de gestion de la circulation ferroviaire)



- Depuis 2017
- Nouvel outil créé spécifiquement par CLEARSY pour ATOS et SNCF
- Amélioration des performances pour gérer les données grande lignes, rajout de nouvelles fonctionnalités : architecture client-serveur et gestion des règles en base de données pour une validation déportée
- Règles supplémentaires développées spécifiquement pour SNCF (client final)

Pour SIEMENS : ATS and ATS+ Parameters (Mainline) : Tool and rules



- Depuis 2018
- Nouvel outil développé par CLEARSY adapté aux besoins Siemens
- Validation formelle de données graphiques (fichiers. ilv)
- Ateliers de définition des règles

Pour THALES : SelTrac CBTC



- Depuis 2019
- Nouvel outil développé pour Thales
- Intégration dans un éditeur de plans de voies
- Développement des règles

Pour ATKINS : Interlocking

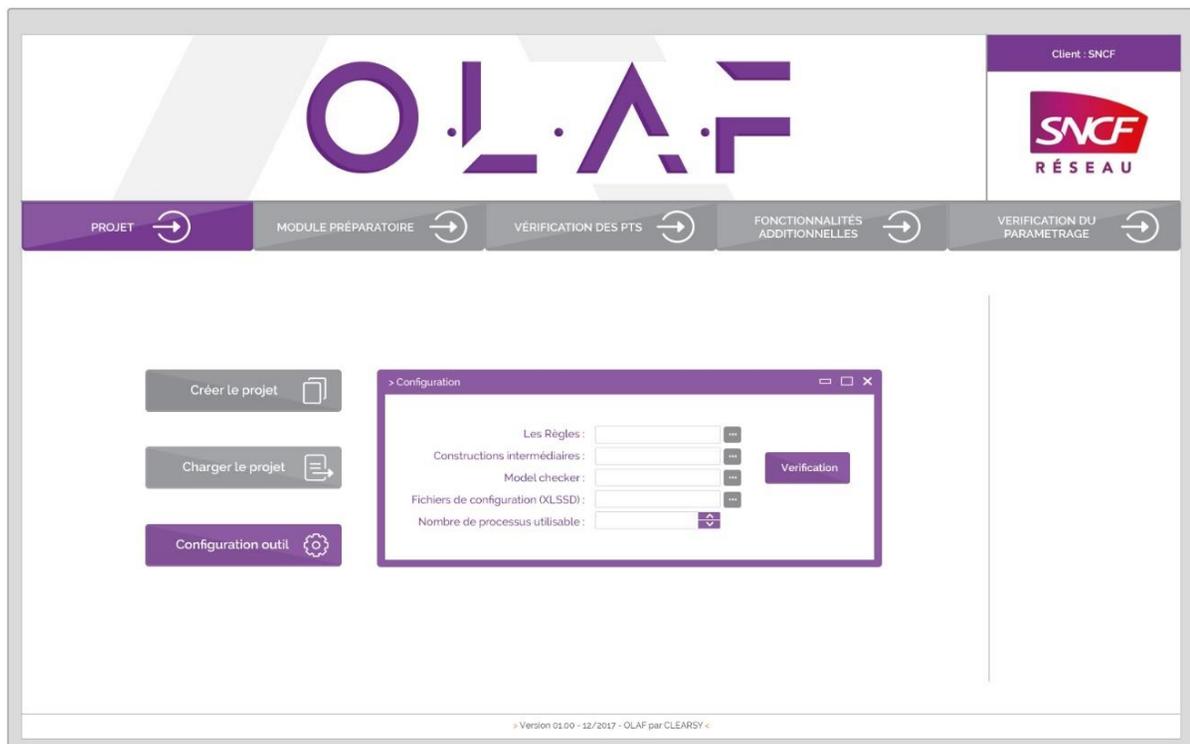


Member of the SNC-Lavalin Group

- Depuis 2019
- Nouvel outil développé pour ATKINS
- Développement des règles

Pour SNCF : données ERTMS (ETCS1)

- Depuis 2018
- Nouvel outil développé par CLEARSY
- ETCS Baseline 2 niveau 1 avec retournement KVB
- Compatibilité des courbes de freinage B3



IHM de l'outil développé par CLEARSY

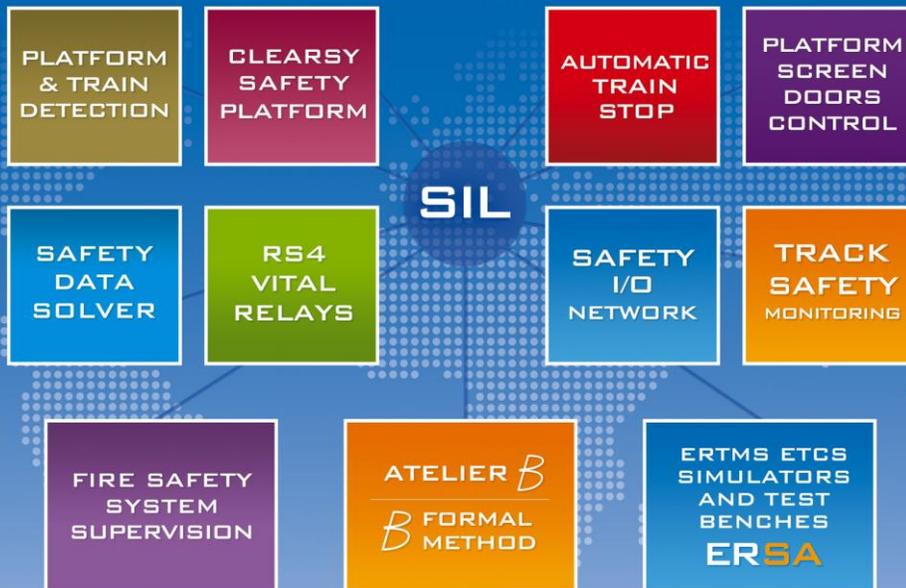
BENEFICES ET RETOURS SUR INVESTISSEMENT

- Augmentation significative du niveau de confiance par l'utilisation d'une solution automatisée basée sur les méthodes formelles.
- Capitalisation des connaissances par la transformation des principes de vérification en règles formelles.
- Vérification complètement automatique et rapide.
- Les outils de validation formelle de données : sont maintenant requis par la SNCF dans les projets type MISTRAL NG, validation des paramètres ERTMS et pour la validation des données ATS+.



CLEARSY

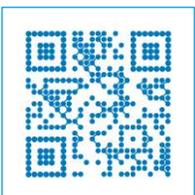
SAFETY SYSTEMS AND SOFTWARE



CLEARSY
SYSTEMS ENGINEERING

WWW.CLEARSY.COM
WWW.FERSIL-RAILWAY.COM

ARTWORK: HULLETTE.COM



- 320 AVENUE ARCHIMEDE
LES PLEIADES III BAT A
13100 AIX-EN-PROVENCE - FRANCE
- TEL. +33 (0)4 42 37 12 70 FAX. +33 (0)4 42 37 12 71
- WEB. contact@clearsy.com / www.clearsy.com