TransForm, Décembre 2017

Institut français
des sciences et technologies
des transports, de l'aménagement
et des réseaux

V&V sur la norme ERTMS/ETCS
Étude des changements de modes

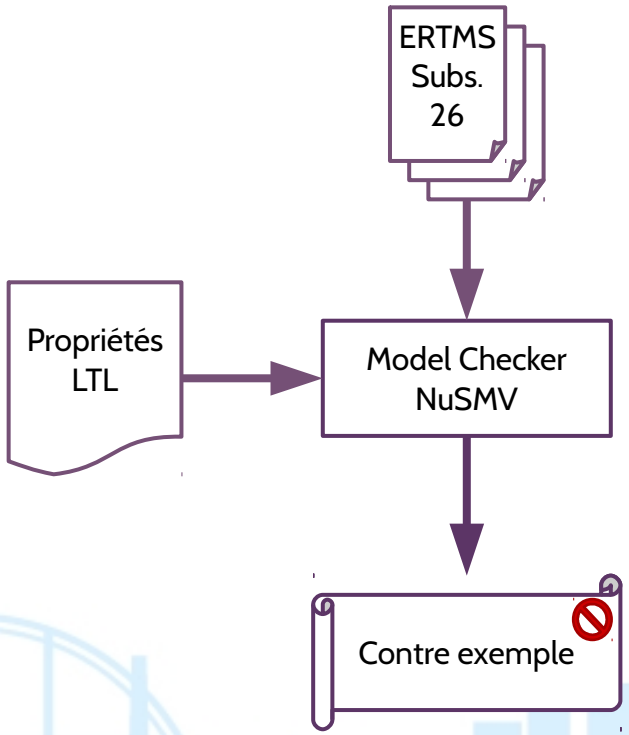
Matthieu Perin, IFSTTAR*
Antoine Ferlin, ONERA (ex IFSTTAR)
Mohamed Ghazel, IFSTTAR

IFSTTAR

IDÉE

Vérification formelle d'ERTMS

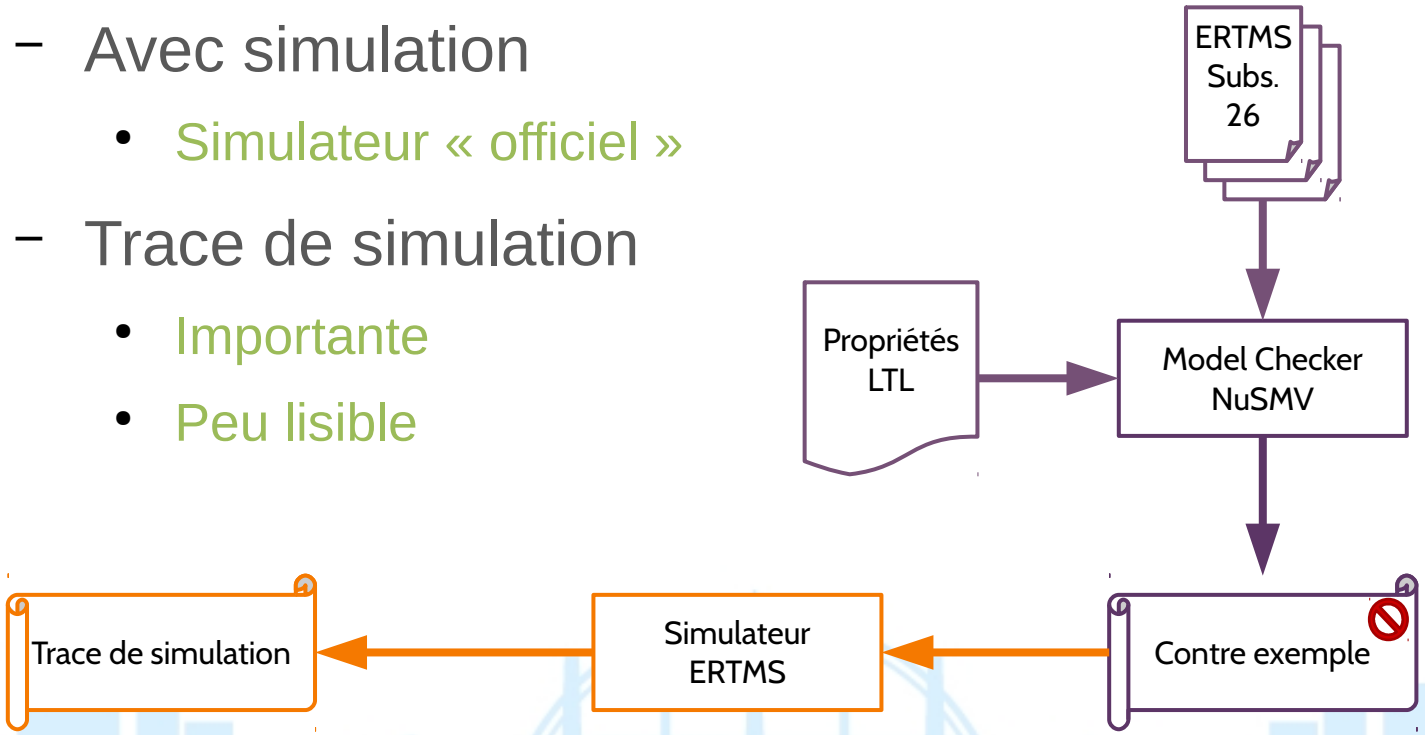
- Cible :
  - Subset 26 & Co
- Comment prouver ?
  - Modèle correcte
  - Propriétés correctes
  - Résultats pertinents



IDÉE

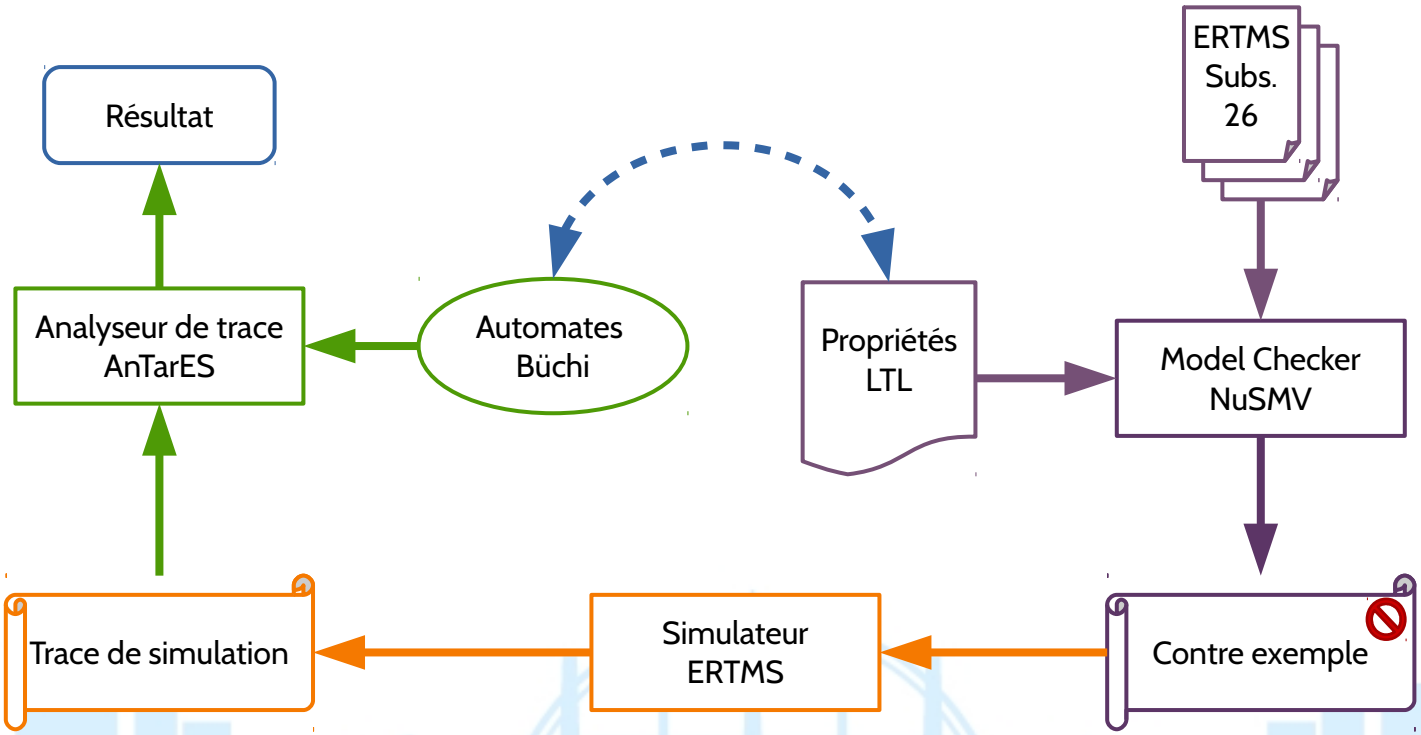
Vérification Formelle d'ERTMS

- Avec simulation
  - Simulateur « officiel »
- Trace de simulation
  - Importante
  - Peu lisible



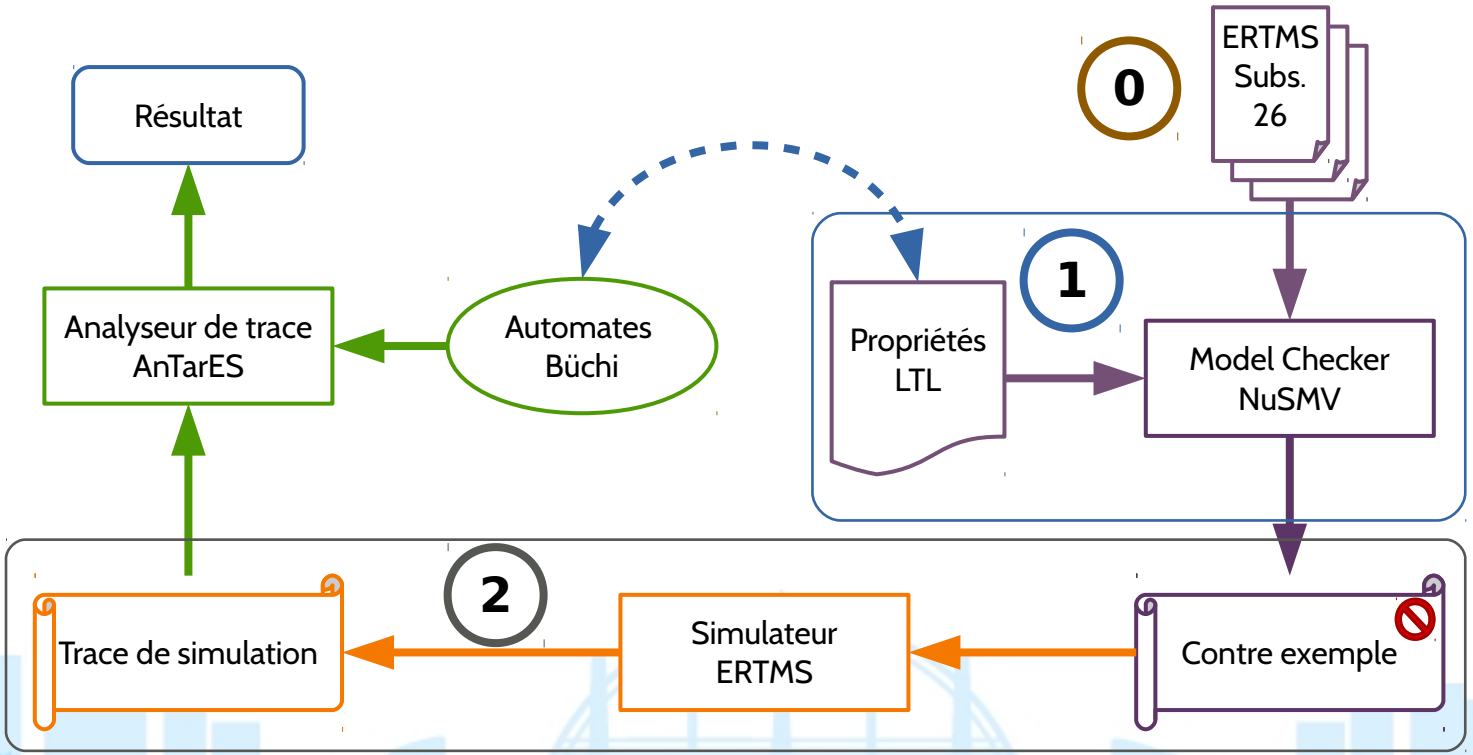
IDÉE

Vérification Formelle d'ERTMS



PLAN

Vérification Formelle d'ERTMS avec V&V



PLAN

0 ERTMS

1 Modélisation NuSMV

- Modèle de changement de mode ETCS
- Propriétés
- Un contre-exemple

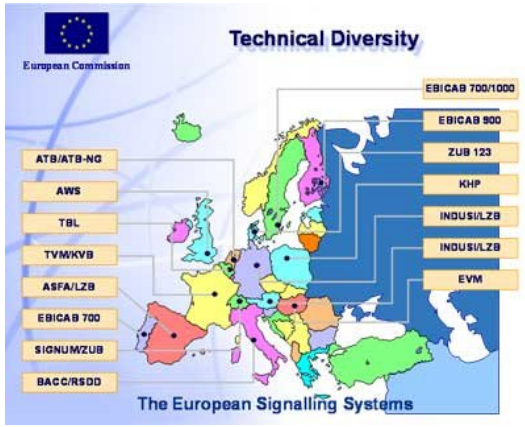
2 Simulation ERTMS

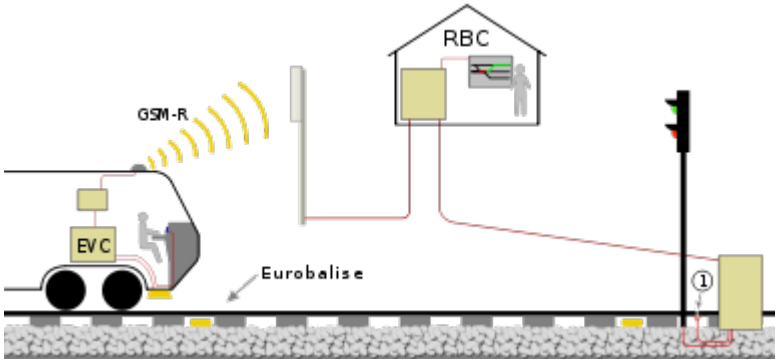
- Production d'un scénario
- Exemple de validation

0 ERTMS : Principes de base

European Railway Train Monitoring System

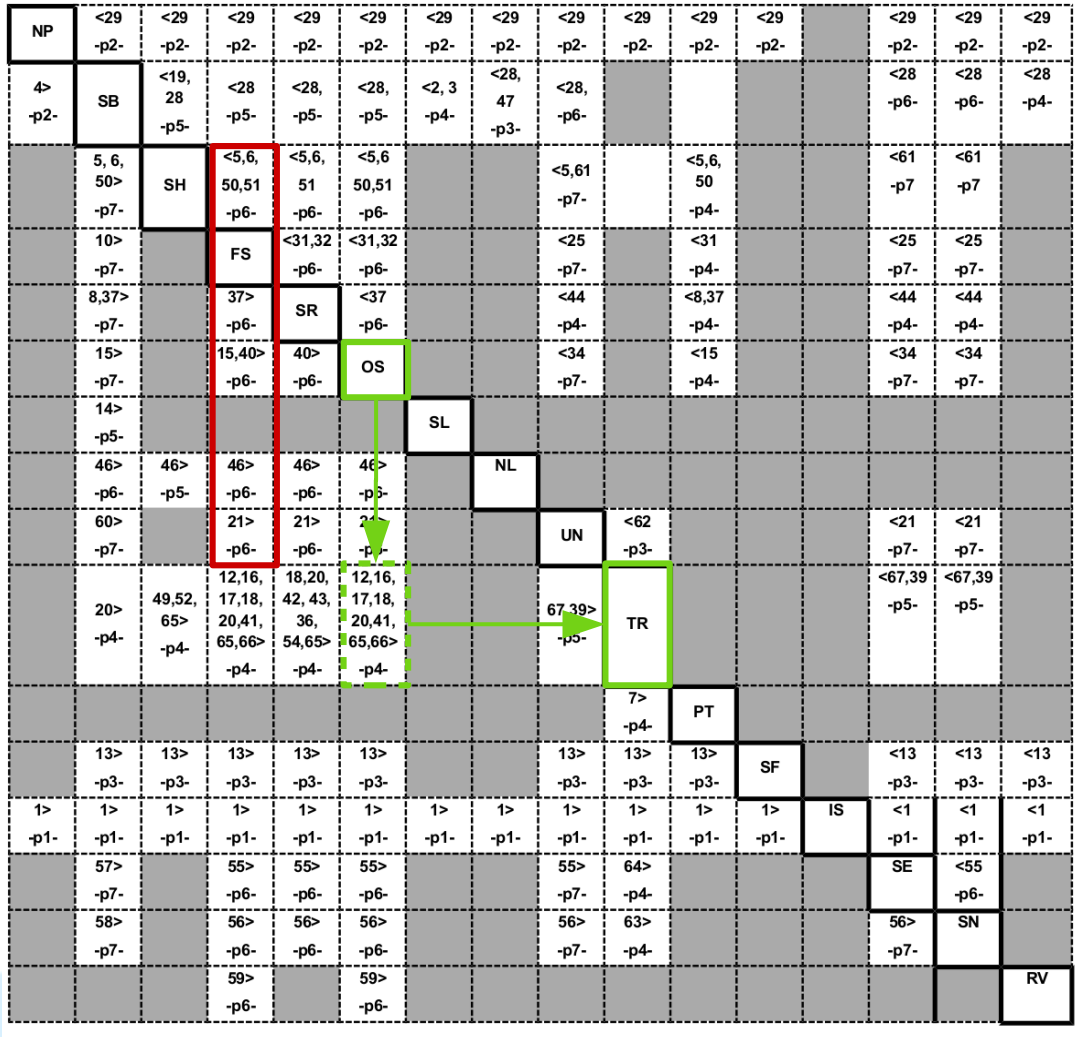
- European Train Control System





0 ERTMS :

Changement de modes



PLAN

0 ERTMS

1 Modélisation NuSMV

- Modèle de changement de mode ETCS
- Propriétés
- Un contre-exemple

2 Simulation ERTMS

- Production d'un scénario
- Exemple de validation

1 Modélisation NuSMV : Présentation de NuSMV

- Système de transition à états finis
  - Basé sur une logique **du futur**
    - Initialisation avec « init »
    - Assignation à la prochaine valeur avec « next »
    - Valeur assignée peut utiliser des valeurs futures !
      - ASSIGN next(bool_a) = next(bool_b) | bool_c
- Model-checker symbolique
  - CTL & LTL

1 Modélisation NuSMV : Modèle du changement de mode

Variables d'environnement

- ETCS

  Powered, desk_open, all_desk_close, ...

- Conducteur

  driver_isolate_EVA, driver_ack_req_SH, …

- À bord

  train_data_onboard, national_trip_procedure, ...

- DMI (IHM)

  SR_proposed_to_driver, ack_req_SH_displayed, …

- Communication

  RCVD_MA, RCVD_trip_order, ...

- Train

  inside_SH, standstill, ...

1 Modélisation NuSMV : Modèle du changement de mode

Changement de mode

- Variable de mode
  - NP, SB, SH, FS, SR, OS, SL, NL, UN, TR, PT, SF, IS, SE, SN, RV
- Système de transition pour les modes
  - Basé sur le tableau de la norme (env. 120 cas)
  - Avec le respect des priorités !
- Ajout de détection d'incohérence
  - Mode spécial FAIL, activé si plusieurs conditions de même priorités sont valables

1 Modélisation NuSMV : Modèle du changement de mode

- Premiers tests : **ÉCHEC !**
- Travail sur le modèle :
  - Variables d'environnement
    - Évolution des niveaux ERTMS
    - Hypothèses de réalisme
      - IHM, conducteur, relations temporelles, ...
  - Variables de contrôle de l'exécution
    - Blocage de niveau ERTMS, suspension de certains contrôles

1 Modélisation NuSMV Propriétés Formelles

Preuves de vivacité

- Tous les modes sont atteignables
  - CTLSPEC EF (mode=SB);
- Toutes les transitions sont réalisables
  - Ex : FS => TR avec condition 12 en level 1
  - CTLSPEC (!EF (

        (mode=FS & conditions_12) &

        EX (EG mode=TR & OBS_level1_all)

    )) ;

1 Modélisation NuSMV Propriétés Formelles

Preuves de cohérence

- Tests de cohérence
  - CTLSPEC !EF (mode=SB & EX mode=FAIL);
- Analyses des traces
  - Dans l'exemple précédent, condition 37 et 50 réalisables simultanément :
    - conditions_37 := driver_selects_override & speed_under_max_limit_for_override;
    - conditions_50 := ack_req_SH_displayed & driver_ack_req_SH;

PLAN

0 ERTMS

1 Modélisation NuSMV

- Modèle de changement de mode ETCS
- Propriétés
- Un contre-exemple

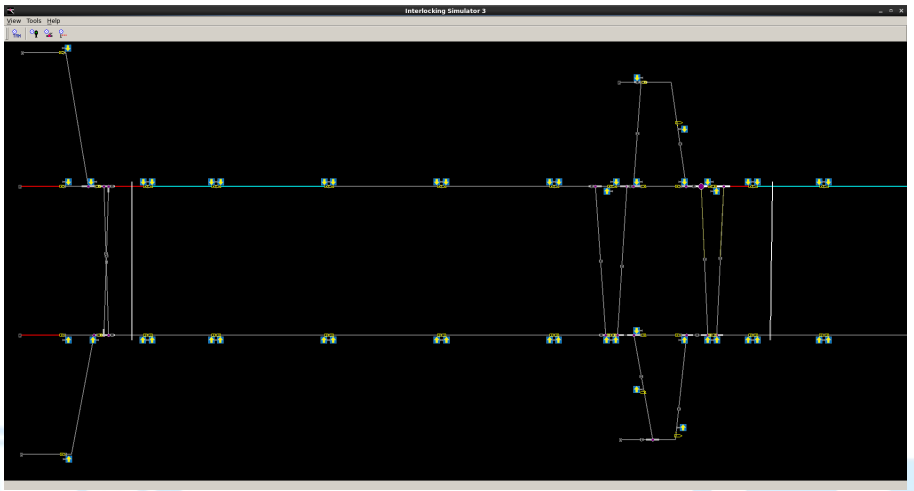
2 Simulation ERTMS

- Production d'un scénario
- Exemple de validation

2 Simulation ERTMS
Le simulateur ERSA

Plate-forme de simulation

- Utilisée pour la conformité des produits industriels
- Simulation
  - Du poste de conduite
  - De l'environnement
- Rendu 3D de la voie



2 Simulation ERTMS
Obtention du scénario

Conception d'un scénario de test

- Basé sur le contre-exemple issue de NuSMV
  - Override & passage SHunting possible simultanément ?
- Sur une voie simple et standard
  - Réalisée dans l'outil
- Le scénario est conçu « à dire d'expert »
  - Et donc lui aussi soumis au risque d'erreur ...

2 Simulation ERTMS Résultats

- Tentative d'override pendant requête de passage en Shunting
  - Impossible car le DMI (IHM) bascule d'un affichage à l'autre
    - Donc validation impossible pour le passage en SHunting
- Bilan
  - Subset 26 pas intrinsèquement sûr !
    - Rattrapé par une autre partie de la norme (DMI)

Annexe AnTarES
Utilisation de l'analyseur de trace

- Pour certaines propriétés formelles
  - Répétabilité, apparitions rares, données temporelles
  - Associées à des conditions de simulation difficiles à reproduire « du premier coup »
- Simulation pour produire des LOG
  - Analyse systématique et formelle
  - Permet d'obtenir des métriques parfois bien utiles
    - Taux de réussite, fréquences d'apparition, ...

Conclusions
Bilan de l'approche

Objectif de vérification formelle d'une norme en langage naturel

- Prouvée par un model-checker
  - Symbolique, CTL & LTL, « constraints-based »
- Utilise de la simulation pour « tester » la pertinence de l'analyse / du résultat
  - Simulateur utilisé en certification
- Utilise un analyseur de trace pour raffiner le résultat
  - Analyse formelle des traces avec métriques

Conclusions
Perspectives

Amélioration de la méthode

- Modèles NuSMV
  - Passer du « constraints-based » au « model-based »
- Simulateur
  - Automatiser au mieux la génération des scénarios
- Analyseur de trace AnTarES
  - Boucle de retour vers NuSMV pour raffinement des propriétés

Merci de votre attention

Ifsttar
Centre de Lille - Villeneuve d'Ascq
20 rue Élisée Reclus, BP 70317,
59666 Villeneuve d'Ascq Cedex
France
www.ifsttar.fr

- Biblio

- Cimatti, A., Clarke, E. M., Giunchiglia, E., Giunchiglia, F., Pistore, M., Roveri, M., Sebastiani, R., Tacchella, A.,2002.
  - Nusmv 2: An opensource tool for symbolicmodel checking. In: Proceedings of the 14th International Conference on ComputerAided Verification. CAV '02. Springer-Verlag, London, UK, UK, pp. 359–364.
- Ghazel, M., 2014.
  - Formalizing a subset of ertms/etcs specifications for verification purposes. Transportation Research Part C: Emerging Technologies 42, 60 – 75.
- Ferlin, A., Wiels, V., Bon, P.,October 2016.
  - Statistical automaton for verifying temporal properties and computing information on traces. International Journal of Computers communications & Control (IJCCC) 11 (5), 645–656.