Title (en)
METHOD FOR CHECKING SAFETY REQUIREMENTS OF SSI-BASED DATA USED IN AN INTERLOCKING CONTROL SYSTEM

Title (de)
VERFAHREN ZUR ÜBERPRÜFUNG VON SICHERHEITSANFORDERUNGEN VON SSI-BASIERTEN DATEN IN EINEM VERRIEGELUNGSSTEUERUNGSSYSTEM

Title (fr)
PROCÉDÉ DE VÉRIFICATION DES EXIGENCES DE SÉCURITÉ DES DONNÉES SSI UTILISÉES DANS UN SYSTÈME DE COMMANDE D'INTERVERROUILLAGE

Publication
EP 3395643 A1 20181031 (EN)

Application
EP 17305477 A 20170428

Priority
EP 17305477 A 20170428

Abstract (en)
Method for checking safety requirements of SSI-based data used in an interlocking control system for controlling an interlocking equipment, the method comprising the steps of: a) obtaining (2) application data representative of interlocking logic operations of the interlocking equipment; b) preparing (4) a constraint violation file containing data representative of a plurality of constraint violation conditions, said data describing a plurality of unsafe scenarios of the interlocking equipment; for each constraint violation condition of the plurality of constraint violation conditions: c) selecting (6) data of the application data according to the constraint violation condition, said selected data corresponding to a predetermined unsafe scenario of the plurality of unsafe scenarios defined in the constraint violation file; d) determining (7) at least one predetermined context associated to said unsafe scenario, said context comprising a plurality of paths through the application data; e) initializing (8) variables that define all possible states of said scenario, thus obtaining a predetermined initial state, said variable being representative of the scenario from the point of view of settings of the interlocking equipment; f) executing (10), starting from said initial state, all possible paths of the context in the application data, thus obtaining respective resulting states; g) at an end of each path, determining (12) if an unsafe state has been reached by comparing a respective resulting state with the data of the constraint violation file; h) if no unsafe state has been detected, determining (12) if the resulting state has not been reached; -i) repeating steps f), g) and h), starting, for each path, from the respective resulting state, until unsafe states or no new states are reached.

IPC 8 full level
B61L 19/06 (2006.01); B61L 21/04 (2006.01); B61L 27/00 (2006.01); G06F 9/00 (2006.01)

CPC (source: EP)
B61L 19/06 (2013.01); B61L 21/04 (2013.01); B61L 27/60 (2022.01)

Citation (applicant)
- MICHAEL HUBER; STEVE KING: "Towards an Integrated Model Checker for Railway Signalling Data", 2002, SPRINGER-VERLAG BERLIN, pages: 20
- SIMON BUSARD; QUENTIN CAPPART; CHRISTOPHE LIMBREE; CHARLES PECHEUR; PIERRE SCHAUS: "Verification of railway interlocking systems", PROCEEDINGS ESSS, 2015

Citation (search report)
- [A] WO 2006111469 A2 20061026 - ALSTOM FERROVIARIA SPA [IT], et al
- [AD] SIMON BUSARD ET AL: "Verification of railway interlocking systems", ELECTRONIC PROCEEDINGS IN THEORETICAL COMPUTER SCIENCE, vol. 184, 1 January 2015 (2015-01-01), pages 19 - 31, XP055419704, DOI: 10.4204/EPTCS.184.2
- [A] N N: "signalling solutions -Smartlock 400", SIGNALLING SOLUTIONS LTD., 31 August 2010 (2010-08-31), Hertfordshire, pages 1 - 16, XP055419677, Retrieved from the Internet <URL:https://signallingsolutions.com/wp-content/uploads/SSL-A4-SL400-Bro.pdf> [retrieved on 20171027]

Cited by
CN116187104A; CN117670630A; WO2024060377A1

Designated contracting state (EPC)
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)
BA ME

DOCDB simple family (publication)
EP 3395643 A1 20181031; EP 3395643 B1 20200311; AU 2018202873 A1 20181115; AU 2018202873 B2 20220519

DOCDB simple family (application)
EP 17305477 A 20170428; AU 2018202873 A 20180426