ANALYSIS

INDUSTRIAL SOFTWARE HOMOLOGATION: THEORY AND CASE STUDY

Guillermo Errezil Alberdi
Formal Vindications S.L. & Guretruck S.L.

In collaboration with:

Joost J. Joosten
University of Barcelona
jjoosten@ub.edu

Gina García Tarrach
University of Barcelona

Aleix Solé Sánchez
University of Barcelona
aleix.sole@ub.edu

Ana de Almeida Borges
University of Barcelona
ana.agvb@gmail.com

Eric Sancho Adamson
University of Barcelona
e.sancho@ub.edu

David Fernández Duque
Ghent University
david.fernandezduque@ugent.be

Download at: http://formalvindications.com/

PURPOSE

Analysis of the European tachograph technology with EU transport Regulations 3821/85, 799/2016, and 561/06 and their consequences for European citizens. The document consists of a comprehensive identification of **bugs**, **problems**, costly **consequences**, **physical impossibilities**, and **legal conundrums** related to this particular marriage between technology and law.

DECENT DESIGN REQUIREMENTS

- **Type1 in Decent Design**: A specification must follow the following logical-mathematical principles and in particular should be consistent: no contradictions are entailed. A desirable additional property is completeness: the system will decide all situations
- **Type2 in Decent Design**: It must respect computational limits (not exceeding available computation time and memory).
- **Type3 in Decent Design**: It must follow physical laws.

WHY DOES THIS MATTER?

The software that generates the tachograph files is proprietary: the source code **is opaque.** The correctness of the tachograph technology and software cannot be checked. However, tachographs are of critical importance in European law enforcement. On the basis of the tachograph files alone, police officers may engage in:

- Penalization with fines (which entails millions in losses for particular truck drivers and companies);
- withdrawal of drivers' licenses;
- incarceration.

In *Industrial software Homologation: Theory and case study* we show **22 well-documented cases** where software errors have caused tangible damage in this domain.

Also, we provide a selection of **31 instances** in the EU in which human intervention was needed to correct erroneous automatic software decisions that led to fines.

Made possible by:
Formal Vindications S.L. & Guretruck S.L. Spanish Ministry of Science, Innovation and Universities, the State Agency for Research and the European Regional Development Fund (ERDF).