openETCS MoU Group

# New Approach for ETCS Onboard Units Based on Open Source Principles


## Summary

***openETCS* is a new approach to specify, design, tender and maintain onboard units for the new European Train Control System to better meet railway undertaking's needs to equip trains in a more economical way. Open standards on various levels, including interface definition and Open Source Software methods are already successfully used in the information and communication technology sector with three major goals: Reducing costs, improving quality and providing greater freedom and independence from equipment suppliers, especially under long term maintenance aspects.**


## Status of the European Train Control System

The European Train Control System (ETCS) is supposed to replace the national legacy signalling and train control systems all across Europe. Especially for the ETCS on-board equipment, the degree of complexity of functions to be implemented is expected to be significantly higher than in conventional systems. In terms of technology, this is mostly done by software in so-called embedded control system implementations. While electronics hardware is getting continuously cheaper, the high complexity of the safety critical software has caused significant cost increases for development, homologation and maintenance of this technology. This has raised questions for many railway operators with respect to the economy of ETCS in general.

Even though six major European suppliers with substantial knowledge in signalling technology have worked on a common System Requirement Specification (SRS) for over a decade, now in its 3rd major revision, the main goal of real interoperability has not been accomplished so far. Up to now, not a single set of onboard ETCS equipment has been approved to operate on all existing European ETCS lines.

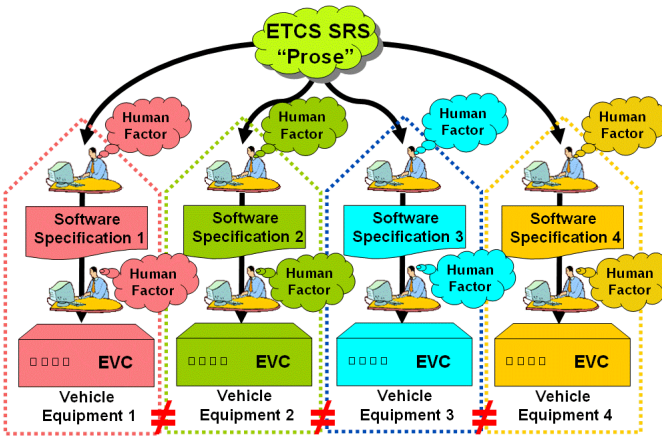
One of the reasons is given by the fact that verbal specification (prose) of some complexity cannot be so precise and free of potential divergent interpretation (Picture 1) that the resulting software products would behave identical under identical operational conditions, which is a prerequisite for EU-wide safe operation. This has caused unplanned costs for subsequent improvement activities.

**Picture 1:**

Divergent interpretation of a common public domain SRS for ETCS, due to the "human factor" by all parties involved, causing different software solutions with deviant behaviour of products from different producers, which result in interoperability deficiencies and costly subsequent improvement activities.

The sector is wasting scarce software R&D resources rather than cooperating on non-USP*) features like subset 026 ETCS core software functions.

*) Unique Selling Point




## Initiative for Finding Alternative Options

Therefore an essential objective for a project initiated by Deutsche Bahn AG is to investigate new options with innovative approaches, in order to bring down equipment costs per vehicle back to the level of conventional train control systems, or even lower. Looking at other industries, such as

automotive promoting a standard computer system architecture called AUTOSAR [1], machine tools industry with open process control like PLCopen [2] and last but not least the aviation sector lead by AIRBUS Industries, which has initiated a project called TOPCASED [3], an open tools suite for specifying, modelling, coding, verifying and validating high assurance software for cockpit control applications. Those experiences could be utilized in the railway.

**Free/Libre Open Source: The European Way !**

A new approach, called "openETCS" has been presented, which intends to define open standards on various levels, like electronics hardware, software, interfaces and tools in order to make use of open concepts to the most possible extend. Essential core part of these standardization efforts is a concept of so-called Open Source Software for both, the final embedded control software product as well as the complete chain of tools for generating software, for verification and validation following the “**Open Proofs**” philosophy [4] (safety case) and providing maintenance as well.

Products which are called "Open Source Software", "Free Software" occasionally "Libre Software", and more often "Free / Libre Open Source Software”, briefly also “FLOSS” [4] is generally characterized by the “Four Freedoms” [6], which allows to

1. Use it for any purpose,
2. Analyze and study the source code,
3. Modify and improve the code, and
4. Distribute the code with or without modifications.

Deutsche Bahn AG, has already gained substantial experience with a large variety of FLOSS applications for office, back-office and web presence including business-critical applications for over an decade. The initial decision for applying FLOSS was mainly triggered by expected savings on license fees, however in retrospective these savings were substantially exceeded by lower quality deficit costs due to better stability, resulting in less down time and lower maintenance costs.

One reason for this is seen in the fact that complex software can practically not be totally free of defects [7]. Despite the relatively short period of practical use of ETCS in revenue service, this has already resulted in a derailment accident in Switzerland [8]. The belief that just extensive testing would be sufficient for a proof of the absence of software faults have already been dismissed back in the 1960s [9], [10]. Only a simple and clear programming style (Edsger W. Dijkstra: “Simplicity is prerequisite for reliability”.) and extended review cycles (Eric S. Raymond: “Given enough eyeballs, all bugs are shallow.” called: “Linus’ Law”: The larger the review team, the better.), are major weapons for high quality safe and secure software products, so called “high assurance software”.

Software engineering practices have shown significant progress in the past 50 years and for the railway sector standards are codified in the CENELEC norms, namely EN50128, and have contributed to well structured software products. However it was not until the Internet offered the possibility of propagating and distributing program source code instantly, inexpensively, in a simple way, and to an almost unlimited extent. This makes software available for a world-wide peer review process for almost all experts in that particular field. Only then FLOSS gained a new quality of options, which cannot be utilized for closed source software.

This global peer-review process has proven to be very effective especially for security-critical faults like “backdoors”. Therefore, the European Union has honoured the value of FLOSS: Resolution **No. A5-0264/2001** of the European Parliament, regarding "… measures to promote self-protection by citizens and businesses" ...:"**The Commission and Member States are called upon to promote software projects whose source text is made public (open-source software)**, as this is the only way of guaranteeing that no ***backdoors*** are built into programmes. The Commission is called upon” …”placing those packages whose source code has not been made public in the '***least reliable***' **category**."[11].

The EU Commission has not only made these recommendations, but has also sponsored substantial research on FLOSS in order to better understand the impact of FLOSS on the EU economy [4].

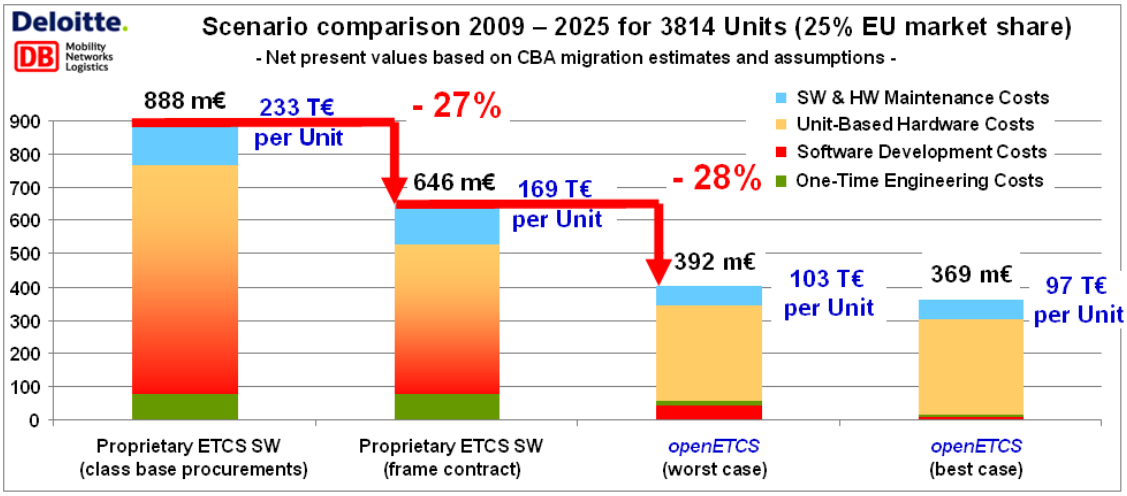
Furthermore the EU Commission has provided a “European Union Public License” [12] in 22 languages, which complies with EU law and the legal systems of all member states. In addition, the European Commission has launched the Open Source Observatory and Repository, OSOR, with the intention of supporting open source software as the epitome of collaborative development of software in the European public sector and has issued a procurement guideline for organizations which have to follow public procurement regulations [13].

Especially FLOSS based projects like TOPCASED have shown that for durable capital goods (aircraft, railway rolling stock) not only the product itself will benefit from FLOSS, but in particular the tools for development, production, and maintenance because their users do not depend any more on individual decisions of firms or their possible withdrawal from the market. On the other hand such programs have demonstrated to attract new resources for research and development which are otherwise not accessible [3].

**Economic Impact of Open Source on the ETCS Program**

As a matter of fact the EU and European governments are increasingly considering the use of Open Source Software as a means of reducing costs, increasing transparency and sustainability, so it would be obvious that such a "European" project like ETCS could tremendously profit from applying FLOSS principles. OpenETCS is such an attempt to utilize the principles of open standards on various levels including open source software.

Based on the results provided by the study called “Economic impact of open source software on innovation and the competitiveness of the Information and Communication Technologies sector” issued by the UNU-MERIT, (NL), DB has sponsored an impact case study on open source concepts applied to ETCS onboard equipment delivered by Deloitte Consulting, Germany, which came to the following results:




Picture 2: Net present value for equipment with proprietary ETCS SW vs. Open Source Software based on 3.814 units (2.873vehicles) assuming a 25% market share of total 11.492 vehicles to be equipped, as reported by 60% of EU railway undertakings, based on differential costs evaluation (without conventional class B system to be integrated).

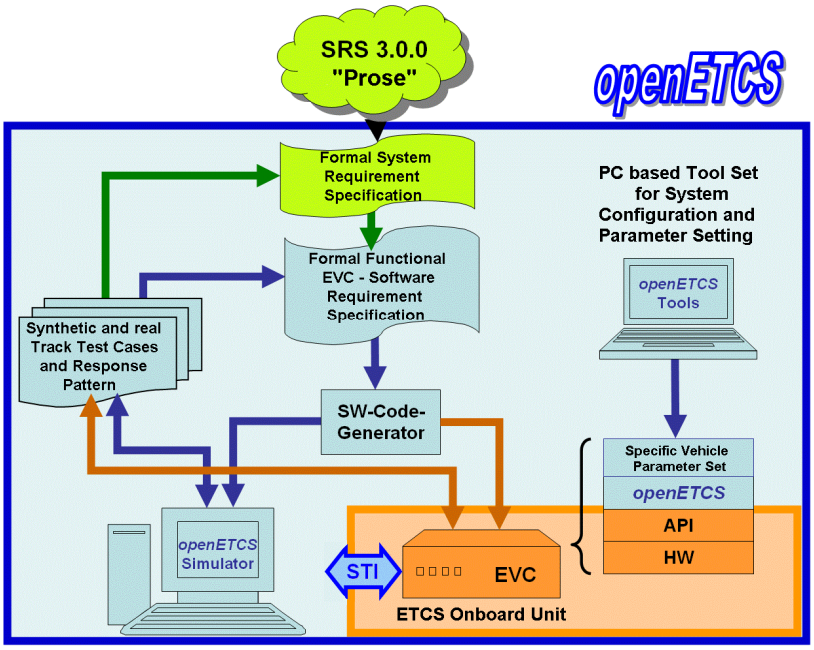
Assuming that 25% of the actual reported demand of ETCS onboard Units by EU railway undertakings for the next 15 years would have been open source licensed, substantial savings on life cycle costs in the order of 500 m€ can be expected, compared to typical conventional single sourced proprietary software, based on per class vehicle procurements, as shown in picture 2 (left bar).

A best case scenario (right bar, full cooperation with EU signalling suppliers and 50% public funding for R&D works within the next 3 years) and worst case scenario (no cooperation with EU signalling industry, external supplier and full private funding) have been evaluated, assuming an open

source consortia business model versus proprietary based products, either within a frame contract or conventionally per class vehicle procurement. While large conventional frame procurement contracts, covering almost 3.000 vehicles, will result in about 27% savings (242 m€), however causing strong dependencies from a single supplier, while an open source business model will result in additional 28% savings (254 m€) by avoiding single source “vendor lock-in” problems for the future.

**Basics of the openETCS Approach**

Since formal methodology is an effective means to avoid ambiguities, the openETCS approach, as shown in Picture 3, includes the formalization of the System Requirement Specification (SRS), published by the European Railway Agency (ERA), as input for an open formal functional software requirement specification document. The SRS will then be the basis for a functional simulation model as well as executable software code for either a Software-in-the-Loop or, later in the process, a Hardware-in-the-Loop-Simulation setup using real production type EVC (European Vital Computer) kernels. Also open test specification data bases, allowing automatic testing, including real life test scenarios for existing track lay-outs and RBC configurations.




Picture 3: Schematics of the "openETCS" project with open components on various levels of the concept.

For comparing various combinations of way-side and onboard units, a non-vital implementation of a functional “EnVC” (European non-Vital Computer, not to be used for revenue service, but test reference only) can be considered as “gold reference standard” and is part of the overall openETCS concept. It also includes the ETCS on-board unit (EVC, HW) requirement specification for a standard train interface (STI), a software interfaces (API: Application Programming Interface) and the actual ETCS application (embedded "openETCS” executable SW) as open source software. A FLOSS-based parameterization and configuration tool assures long-term maintainability of the embedded EVC software. It is essential to cover the whole life-cycle from specification over code generation (e.g. trusted compilers [14], [15]), verification and validation tools required as FLOSS in order to guarantee system integrity, also called “open proofs” [4] for providing “high assurance” to meet the essential safety and security requirements for public transportation systems.

**Almost none of the openETCS components have to be developed from scratch.**

Most of these components are already available within the supplier community, sub-suppliers or test lab organizations, so that this program is mainly a question of cooperation, legal and marketing issue, rather than a question of different engineering methods. Even most of the components

needed for the openETCS tools chain are available in open source licensed versions, just requiring adaptation to the railway sector. That means, with the exception of concise formal specification documents for the SRS, software and test cases and an open sourced test bench software itself, which are not yet on the market in a sufficiently high quality, almost all other components are already more or less available and need only to be migrated from proprietary into FLOSS.

The whole migration process can be exercised step by step: First providing a non-vital reference ETCS onboard unit, based on formal specification methods, to be used as a neutral "golden item" helping all parties to secure full interoperability, then providing open source test benches and finally acquiring intellectual property (IP) of already service proven production type vital ETCS onboard software from one supplier and converting it into FLOSS, providing a common "standard" ETCS software kernel to the entire sector to be used in various ETCS OBU hardware products.

**Cooperation between competing partners in the railway sector.**

It is well understood that such a change cannot be accomplished even by the largest railway undertaking alone. Therefore several EU railway organizations, as there are: ATOC (UK), DB (D), NS (NL), and SNCF (F) have already signed a Memorandum of Understanding promoting the openETCS concept, by supporting FLOSS based ETCS project activities.

**References:** (Internet Ref. Status: 01.03.2011)


[1] AUTOSAR (AUTomotive Open System ARchitecture); http://www.autosar.org/

[2] PLCopen; Molenstraat 34, 4201 CX Gorinchem, The Netherlands,: http://www.plcopen.org

[3] TOPCASED: The Open Source Toolkit for Critical Systems; http://www.topcased.org

[4] Open proofs: http://www.openproofs.org/wiki/Main_Page

[5] *UNU-MERIT, The Netherlands (Lead contractor):* Economic impact of open source software on innovation and the competitiveness of the Information and Communication Technologies (ICT) sector http://ec.europa.eu/enterprise/ict/policy/doc/2006-11-20-flossimpact.pdf

[6] *Free Software Foundation, Inc.; 51 Franklin Street, Boston, MA 02110-1301, USA:* http://www.gnu.org/philosophy/free-sw.html,

[7] *Ostrand, T. J. und andere:* Where the Bugs Are. In: Rothermel, G. (Hrsg.): Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis, Bd. 29, 2004, S. 86ff

[8] *Schweizerische Eidgenossenschaft, UUS:* Schlussbericht der Unfalluntersuchungsstelle Bahnen und Schiffe über die Entgleisung von Güterzug 43647 der BLS AG vom Dienstag, 16. Oktober 2007, in Frutigen. http://www.uus.admin.ch//pdf/07101601_SB.pdf

[9] *Randell, B.:* The NATO Software Engineering Conferences, 1968/1969: http://homepages.cs.ncl.ac.uk/brian.randell/NATO/

[10] *Dijkstra, Edsger W.:* The Humble Programmer, ACM Turing Lecture 1972. http://www.cs.utexas.edu/users/EWD/ewd03xx/EWD340.PDF

[11] *Europäisches Parlament:* Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation, Aktenzeichen: A5-0264/2001, 11. Juli 2001. http://www.europarl.europa.eu/ (or google for „A-0264/2001")

[12] *European Commission, IDABC:* European Union Public Licence - EUPL v.1.1 Jan. 9, 2009. http://ec.europa.eu/idabc/en/document/7774

[13] OSOR Guideline on Public Procurement and Open Source Software - public draft v1.0, http://www.osor.eu/idabc-studies/OSS-procurement-guideline-public-draft-v1 %201.pdf

[14] Ken Thompson: Reflections on Trusting Trust; Reprinted from Communication of the ACM, Vol. 27, No. 8, August 1984, pp. 761-763. http://cm.bell-labs.com/who/ken/trust.html

[15] Wheeler, David A.: Countering the Trusting Trust through Diverse Double-Compiling (DDC)…, http://www.dwheeler.com/trusting-trust/



**Contact:**

Klaus-Rüdiger Hase
openETCS MoU Group
Mail: mail@openETCS.eu

**Address:**

c/o Deutsche Bahn AG
Richelstrasse 3, D-80634 München, GERMANY