Software in Railway Applications



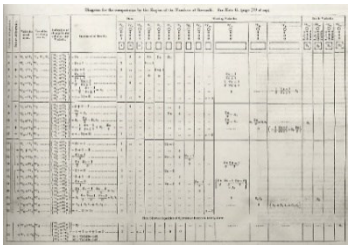
In this modern era, software is embedded in all aspects of our life. Without software, our lives would be completely different. Can you imagine your typical day without a smartphone or laptop? Even in our cars and trains, software is essential to functions and services for both drivers and passengers. So, what is software? How do we ensure it is fit for its intended use? And, how do standards help us do this?

Lucia Capogna answers these questions, provides an overview of software standards in rail and their evolution, and discusses the latest developed software standard for railway applications. Lucia will explain the significant changes, the additional guidance on lifecycles and model-based design and how some requirements have been rewritten to aid interpretation and understanding. She has also interviewed two members of the CENELEC WG28 on their thoughts about the new software standard and the future of software.

Note: the first part of this paper provides background for those less familiar with software and the current railway standards for software; the second part covers recent developments in more detail.

Software – history, definition and main characteristics

The first electronic stored-program digital computer was realised in 1951 with the Electronic Discrete Variable Automatic Computer (EDVAC). The idea of programming was first established over 100 years earlier in 1843, when Ada Lovelace (who worked closely with Charles Babbage) published the first computer program (an algorithm to calculate a sequence of Bernoulli numbers).



Ada Lovelace is still considered the founder of the discipline. The first person that really came up with a software theory was Alan Turing in 1935, and it is from there that both computer science and software engineering disciplines originated.

Since then, software started becoming popular and making inroads everywhere including the railway industry. But what is software?

The International Electrotechnical Vocabulary (IEV) [12] defines software as:

"assembly of programs, procedures, rules, documentation and data, pertaining to the operation of an information processing device or system.

Note 1 to entry: Software is an intellectual creation that is independent of the medium upon which it is recorded.

Note 2 to entry: Software requires hardware to execute programs, and to store and transmit data."

"Software requires hardware to execute programs, and to store and transmit data."

(Note 2 of IEV ref 171-01-21)

Software is something intangible (it cannot be hit by a hammer) that does not exist alone and, for this reason, it cannot cause damage on its own. It has a large list of advantages including flexibility and scalability, cost-effectiveness, fast response to issues and it is indefinitely replicable (cheap) especially on large scale projects where it can be uploaded and changed on multiple systems in parallel. However, software is context dependent, can have a large number of failure modes and it is impossible to test exhaustively (it cannot be demonstrated to be 'bug' free).

The need for a structured approach

As you may know, software is subject to systematic failures only, so a qualitative approach must be considered.

Software has gradually changed the face of railway as numerous command systems, both safety and non-safety related, have been innovated, become more flexible and evolved thanks to the use of software.

Over the years, in the Rail industry, as well as other industries with safety critical control systems, we have seen incidents caused by software failures. How do we ensure the software is fit for its intended use? In particular, how do we do it for safety related software?

Root cause analysis and incidents investigations have identified poor management in several areas across the software lifecycle starting from the requirements management, testing, verification and validation, but also lack of recording and management of change. More guidance and a more structured approach for software assurance was needed through further standardisation, and adoption of improved procedures and guidance. The more general importance of standards has been discussed in more detail in the SSS'23 paper "Making the Safety Standards Work for You" [1].

Rail Software Standards – Their history

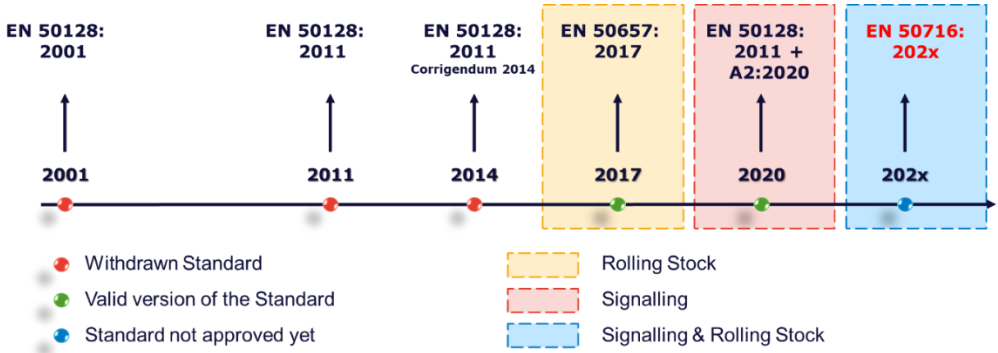
To answer the need of having common rules when developing software for railway applications, a group of experts representing different stakeholders across the rail industry and several European countries, worked together to create the first software standard for railways applications: "EN 50128:2001 – Railway applications - Communication, signalling and processing systems – Software for railway control and protection systems" [3].

This standard follows a top-down approach to identify suitable methods for software development depending on the integrity required. It addresses 5 software integrity levels, SIL 0 to SIL 4, where 0 is the lowest and 4 the highest. The higher the risk resulting from software failure, the higher the software integrity level needs to be.

This standard has been gradually adopted by the industry and stayed unchanged for 10 years, until an updated version of the same standard was developed and published (EN 50128:2011). The 2011 version has been greatly improved thanks to the return of experience from the industry; it has adopted a new structure that has remained stable since then.

For over 16 years the EN 50128 (in its different versions) has been the software standard used by both Signalling and Rolling Stock, despite the fact it was specifically developed for signalling and protection systems. However, in 2017 a dedicated software standard for Rolling Stock was published: "EN 50657:2017 – Railways Applications – Rolling stock applications – Software on Board Rolling Stock" [5]. The EN 50657:2017 adapted EN 50128:2011 requirements for the application of software in the Rolling Stock domain and aligning it to the principles and terminology used in the new EN 50126 series [9]. [10] (published in the same year, 2017). From now on SIL 0 is replaced with Basic Integrity (BI).

TC9X WG28 received the mandate to update EN 50128:2011 [4] to align with other standards in the railway framework (i.e., EN 50126-1:2017 [9], EN 50126-2:2017 [10] and EN 50129:2018 [11]) resulting in the EN 50128:2011 + A2:2020 [6] published by The British Standards Institute (BSI) in August 2020. This has been a first step towards the development of a new software standard applicable to both Rolling Stock and Signalling: FprEN 50716 [7]; this standard is currently under final vote and it is expected to be formally published before the end of 2023.



FprEN 50716 Improvements and changes – Open discussion with key people in the CENELEC Standardisation group (WG28)

The FprEN 50716 standard [7] will supersede the latest EN 50128:2011 [6] and EN 50657:2017 [5] and all of their amendments and corrigenda, hence it is applicable for both Signalling and on-board Rolling Stock. For railway related fixed installations (electric traction power control and supply) "EN 50562:2018 - Railway applications - Fixed installations - Process, protective measures and demonstration of safety for electric traction systems" [8] remains applicable.

FprEN 50716 [7] includes several significant technical changes with respect to the latest EN 50128:2011 [6] and EN 50657:2017 [5]. The new software standard is now fully aligned with EN 50126-1:2017 [9] and EN 50126-2:2017 [10] terminology and definitions, and many requirements have been re-written to simplify and clarify them (e.g. organisation requirements); the techniques and measures have been better aligned with the lifecycle phases, and generalised where appropriate (e.g. programming languages). This standard now offers guidance on several lifecycle models and on modelling for software development as many software projects are now using modelling and model-based design. The emerging use of Artificial Intelligence (AI) and Machine Learning (ML) is also discussed and recommendations and guidance from a previous version of EN 50128 have been reviewed and updated in the new standard. Although many areas have been improved or added, the core requirements of the existing software standards stayed nearly unchanged. Those requirements are already clear and left untouched as they are good principles across the software development processes.

The author interviewed Andrea Palermo and Attilio Ciancabilla to discuss the changes introduced in the FprEN 50716 [7], the challenges faced when developing the new standard and the future of software in railway applications.

Andrea Palermo is the Convenor of WG28 for the new FprEN 50716 [7] (UK National Committee). He is also involved in other CENELEC and IEC safety standardisation working groups. Andrea works in Thales GTS, defining digital solutions for the UK mainline railway.

Attilio Ciancabilla is an active member of WG28 for the new FprEN 50716 [7] (IT National Committee). He is also involved in other CENELEC and IEC safety and cybersecurity standardisation working groups. He is the convenor of WGA15, in charge of maintenance of EN

50129. Attilio works in RFI (Rete Ferroviaria Italiana) in the signalling field, mainly for electronic interlocking systems.

I asked Andrea, what it meant for him to lead the group developing a new software standard to be used for both Rolling Stock and Signalling, and what challenges / rewards he had from the experience but also if he would change anything that has been done.

Andrea said that the 2001 version of EN 50128 really transformed the way software was developed for signalling applications and through the years became a best practice used for overall assurance (beyond safety) and cross domain, so when a mix of experts started working together on the FprEN 50716 [7] they all had a common language and understanding! Andrea also clarified that it was immediately clear that while the majority of needs were common, significant differences existed: his role was to lead the group in finding the right compromises.

One of the biggest challenges for Andrea was to lead the group during the COVID-19 pandemic, however he has seen this "low" point as an opportunity to "virtually" work together more frequently than what would have been possible with in-person meetings, transforming it into a "high point". Andrea went through the steps made in the last few years, from the work done in the survey group that produced a baseline draft merging EN 50128 [6] and EN 50657 [5] with agreed trade-offs between all experts and explained that this impacted on the direction the standard has taken. After that, the "mantra" of the working group was to keep continuity from EN 50128 and EN 50657 and facilitate transition – they even kept the majority of the numbering of clauses unchanged in this respect to minimise traceability updates. The choice was made consciously, but he underlined that if they would have gone for a thorough review from first to last page, the standard would have been much different.

I asked both Attilio and Andrea their opinion on the direction the software standard is taking and their thoughts regarding the use of new "technology" or "approaches" like AI and ML and how standards may need to evolve to accommodate cloud-based solutions.

The standard kept the usage of AI and its derivatives like ML open for basic integrity (it is not recommended for SIL 1 – SIL 4) but Andrea expects that in the coming years, these techniques will be used also as sorts of "support tools" to gain additional confidence in software verification and validation (the standard does not preclude this as it defines the "what" not the "how" in term of development process). The next revisions of the standard will probably expand on AI topics over the coming years, also taking benefits from the broader standardisation efforts on-going in IEC/CENELEC.

Overall, both Andrea and Attilio agreed that merging the two existing standards into one has been a great achievement considering the different needs, but also, that we work in an integrated context. Attilio has a long history in the standardisation environment, and he is quite sure that in a not-too-distant future we will be able to extend the standard to fixed-installation applications as well.

"Leading the WG28 was such an enriching experience! {..} finding the right trade-offs has been probably the most rewarding part of the work."

Andrea Palermo (Convenor of WG28)

Attilio said that, in his opinion, another big improvement has been simplification: requirements on roles have been clarified, approach to programming languages was obsolete and has been changed. In general, we can say that the standard is now more flexible and less constraining, which will make it easier to use.

Attilio also said that cloud computing is in our future. Railway applications are characterised by relatively slow real time processes, so he does not think it will be difficult to guarantee high available, fail-safe and secure cloud computing. But for adequate fault tolerance he also believes that there will be a need for some local element able to manage the so-called "graceful degradation", and this architectural challenge will perhaps be the most difficult to solve.

At the end of this interesting discussion, I asked Attilio what he thinks will be the impact of this new standard on the industry also considering its relationship with other existing standards like EN 50126, EN 50129 and the TS 50701. Attilio said that it is always difficult to consider the relationships between standards and their inter-applicability and despite the great work that has been done to align the EN 50716 to the EN 50126 and EN 50129, there is still room for improvements (e.g., requirements on tools). He concluded that differently from EN 50129 and from the latest EN 50128:2011 [6], this new software standard will extend the scope to non-safety-related software. Attilio is afraid there will be some resistance in adapting to this, but on the other hand this will facilitate the homogenisation of developing processes and will eventually be seen as an advantage.

Cambrian Coastline incident and RIS-0745-CCS

The Railway Industry Standard RIS-0745-CCS [12] has been produced by The Rail Safety and Standards Board (RSSB) to support Network Rail (after the Cambrian incident [2]) and the rail industry in general. It gives guidance and sets requirements regarding safety assurance activities for the client's organisation responsible for the procurement and use of safety-related software-based systems. It heavily refers to the EN 50126/8/9 standards. The client's role in safety assurance is defined at the level of the whole system under consideration. When a high integrity software-based system is procured, the client organisation is the relevant Railway Duty Holder under the relevant regulations.

The focus of this standard is to ensure that the software within high integrity software-based railway systems does not cause hazards and it is less focused on the in-depth analysis of the actual activities to develop and maintain safety-related software-based systems. The RIS-0745-CCS [12] clarifies the responsibility of the client organisation in meeting the requirements of the suite of railway software standards; it provides them with increased confidence that the requirements of the suite of railway software standards and the CSM-RA (Common Safety Method for Risk Evaluation and Assessment) have been met by requiring further specific activities.

Conclusions

An increasing portion of the railway functions (safety and non-safety related) are being supported by software.

The risk associated with the use of software in the safety context has led to the need for more guidance, procedures and standards to increase the quality of the software and to assure that the risk is reduced to a tolerable level.

The newly developed cross-domain standard (FprEN 50716 [7]) improves readability of the requirements and gives more guidance on several aspects compared to the two existing software standards it will supersede (EN 50657 [5] and EN 50128 [6]). It is also more flexible and less constraining, which will make it easier to use.

"The role of a standard such as EN 50716 is to follow innovation, providing minimum requirements on objectives and processes.

Attilio Ciancabilla
(Convenor WG15 and member of WG28)

Software is so embedded in railway functions that the RSSB created an industry standard to support software assurance from the client perspective (RIS-0745-CCS [12]) aiming to reduce risks associate with its use.

Compliance to standards gives reassurance and increases confidence that the software is fit for its intended use and that its quality is adequate for the identified safety integrity level. These methods support a structured and consistent approach in the development, verification and validation of the software and its use across different organisations and countries.

References

[1] SSS23 Bull, Capogna, Davies & Gill – Making the Safety Standards Work for You, Feb 2023

[2] RIAB, Dec 2019, "Loss of safety critical signalling data on the Cambrian Coast line, 20 October 2017".

[3] CENELEC, EN 50128:2001, Railway applications - Communication, signalling and processing systems – Software for railway control and protection systems

[4] CENELEC, EN 50128:2011, Railway applications - Communication, signalling and processing systems – Software for railway control and protection systems

[5] CENELEC, EN 50657:2017, Railways Applications – Rolling stock applications – Software on Board Rolling Stock

[6] CENELEC, EN 50128:2011 + A2:2020, Railway applications - Communication, signalling and processing systems – Software for railway control and protection systems

[7] CENELEC, FprEN 50716, Railway applications - Requirements for software development

[8] CENELEC, EN 50562:2018, Railway applications - Fixed installations - Process, protective measures and demonstration of safety for electric traction systems

[9] CENELEC, EN 50126-1:2017, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

[10] CENELEC, EN 50126-2:2017, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety

[11] CENELEC, EN 50129:2018, Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling

[12] RSSB, Rail Industry Standard, RIS-0745-CCS, Client safety assurance of high integrity software based systems for railway applications

[13] https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=171-01-21, accessed, Sep 2023

Image attribution
top image ID 210738093 © BiancoBlue | Dreamstime.com
Diagram for the computation of Bernoulli numbers © Public Domain | https://en.wikipedia.org
Standards Timeline © Lucia Capogna

Lucia Capogna, Principal Engineer, Ebeni Limited

Lucia has over 15 years' experience in software, safety and cyber security with background in multiple industries including Railway, Defence, Oil & Gas and Renewable Energy. Lucia also represents the UK in several CENELEC and IEC standardisation groups (UK NC) for software, cybersecurity and safety standards, including WG28 (FprEN 50716).