Acta Polytechnica CTU Proceedings **43**:1–5, 2023
https://doi.org/10.14311/APP.2023.43.0001

INTEGRAL RAILWAY INTERLOCKING SYSTEM AND ITS ASSESSMENT ACCORDING TO EUROPEAN STANDARDS

Tomáš Brandejský[a], Vít Fábera[a,*], Martin Leso[b]

[a] *Czech Technical University in Prague, Faculty of Transportation Sciences, Department of Applied Informatics in Transportation, Konviktská 20, 110 00 Prague 1, Czech Republic*

[b] *Czech Technical University in Prague, Faculty of Transportation Sciences, Department of Transport Telematics, Konviktská 20, 110 00 Prague 1, Czech Republic*

[*] corresponding author: fabera@fd.cvut.cz

Abstract. This paper analyses the component of the Integrated Interlocking System which forms the central logical and functional unit implementing all logical and computational functions necessary for railway traffic control in the Railway 4.0 concept. The main principle is that this approach centralizes the technology of station interlocking system, track line interlocking systems, level crossing interlocking systems and the functions of train interlocking system – the line part of ETCS L2/3 radio block control panel (RBC). The operation control is centralised to the controlling dispatcher centres.

The paper discusses the concept of integrated interlocking system including safety issues addressed from the perspective of the requirements of CENELEC standards EN 50126, EN 50128 and EN 50129. These requirements are addressed from the perspective of the authors of the paper, who also work as independent assessors of the safety of railway control and command systems.

Keywords: Integrated interlocking system, cloud, European standards, EN 50126, EN 50128, EN 50129, assessment.

1. Introduction

The current architecture of interlocking systems, including the implementation of ETCS, is nowadays mainly solved by locally (decentralised) technologies, which require relatively significant requirements for their construction and operation (Figure 1). It is necessary to build a lot of technological buildings, which include backup power sources, air conditioning units, etc.

The Railway 4.0 concept was introduced in [1]. As it has already been explained in those paper, the majority parts of railway infrastructure, especially outside the TEN-T railway corridor with a length of about 7000 km of track lines, is constituting almost 2/3 of the railway network of the Czech Republic. These tracks often contain a lot of railway stations with a small number of stations track lines and a large number of level crossings on the tracks. These track lines are also single track, which has a major impact on the lack of capacity. The Railways 4.0. concept discusses the possibility to combine distributed signalling technology with centralisation of logical and computational parts (integral interlocking system). It makes possible to reduce the number of external technological buildings and replace them with distributed OC object controllers. Controlling and commanding of these external technologies is centralised in the integrated signalling system of the IZZ, which is further interconnected with the central control centres of the CDP. The GSM-R digital radio system, consisting of the MSC master controller and the distributed BTS base stations, DM (Digital modul of GSM-R) are also parts of the whole digital railway control system. The whole digital railway system requires high quality high capacity transmission lines consisting of fibre optic cables (Figure 2).

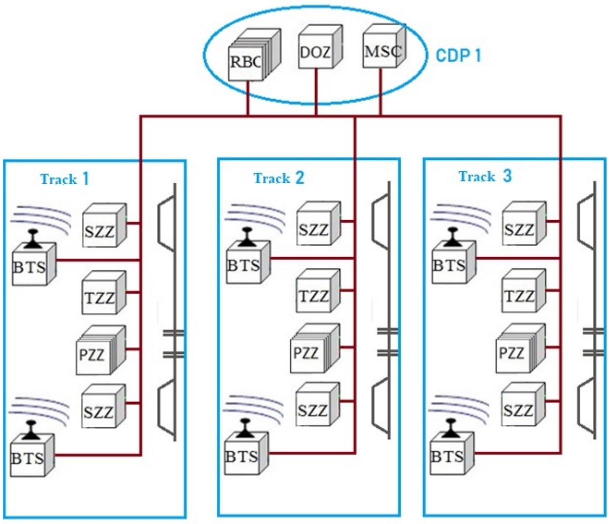

Figure 1. Standard architecture of decentralized railway interlocking system.

2. Integral interlocking system

The main principle of this approach is to centralize the technology of station interlocking system SZZ (setting up train and shunting routes in stations), track

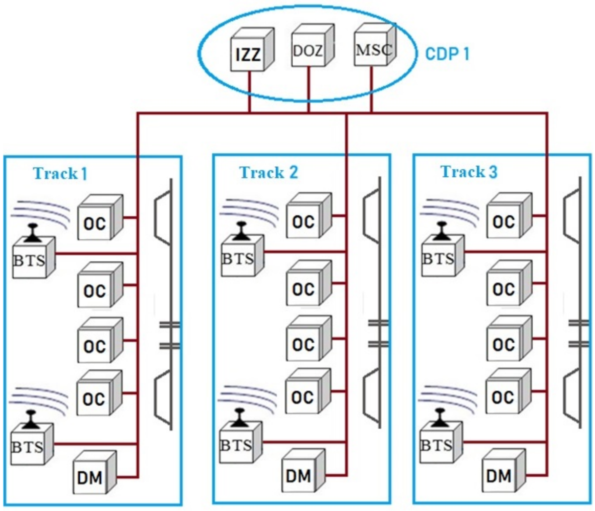

Figure 2. New architecture of integral railway interlocking system.

line interlocking systems TZZ (commanding the movement of trains on the line), level crossing interlocking systems PZZ (ensuring the safety of level crossings) and the functions of train interlocking system – the line part of ETCS L2/3 radio block control panel (RBC). The one way how to make a centralization is to implement the whole system in cloud. This concept has been already produced be several manufacturers and deployed [2–4]. Some producers designed own proprietary solution (like DS3 platform from Siemens Mobility GmbH [5]) others try to use cloud solution based on COTS (like TAS platform from Thales Austria GmbH [6]).

The architecture of IZZ realized in the cloud is shown in Figure 3. The solution brings many advantages. Cloud is a system of tightly knit physical servers, switches and other devices (see Section 2.2) that act as one highly performant and highly available computational platform. The cloud allows the parallel execution of a large number of instances of individual applications implementing logical and computational algorithms for railway traffic control. These applications have a similar logic and function to current technologies (PZZ, SZZ, TZZ, RBC), but their functions (range of functions, specific parameters and settings) are modified through a defined configuration – they are configured with data from the configuration memory (memory protected against random overwriting) during their initialization. IZZ with cloud technology also provides communication with remote OC object controllers via HW and SW resources over optical networks via IP protocol with very high level of security and safety. The additional consequence of centralization is cost reduction for building local technologies and their maintainance cost because local technologies are reduced to object controllers (OC). But using the cloud solution defines new problems and requirement to satisfy European standards (architecture, communication with object controllers).

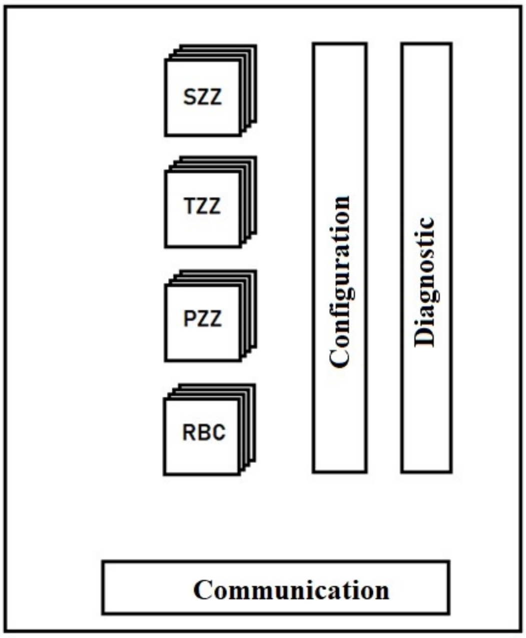

Figure 3. Architecture of railway interlocking system in cloud.

2.1. European standards

The solution must be designed to satisfy European standards EN 50126, EN 50128, EN 50129 (Figure 4). The standards EN 50126 [7, 8] define the life-cycle of the system and gives the instructions to guarantee RAMS parameters: R – Reliability, A – Availability, M – Maintainability, S – Safety. The standard EN 50128 [9] defines requirement for software development (software lifecycle). The EN 50129 [10] contains requirements for architecture of hardware and guidelines how to evaluate reliability. The standard EN 50159 speaks about communication systems. Moreover, security must be considered as well, although standard EN 50701 for cybersecurity is under preparation process.

2.2. Clouds

Cloud is perceived as system to store personal data, photos or provide hosting for web based applications by public. More specifically, the cloud is a group (cluster) of computers (servers) working in data center. The cloud technology is based on *virtualization*: the special virtualization software runs on physical computers (host computers) and allows existences of independent virtual computers *(Virtual Machine – VM)* with own operating system and applications. The virtualization software that creates, runs and manages virtual machines is called *hypervisor*. The one of basic architecture of host with virtual systems is in Figure 5.

There are two types of clouds: *public* and *private* clouds. In the case of public cloud (Microsoft Azure, Google Cloud) users share hardware (physical computers, storage) through virtual computers with other

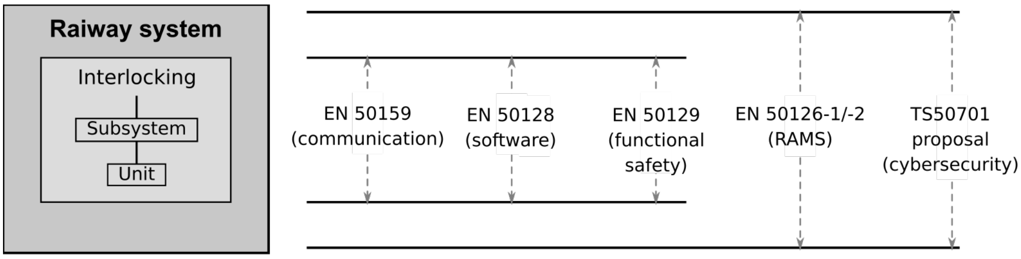

Figure 4. Interlocking system and European standards [11].

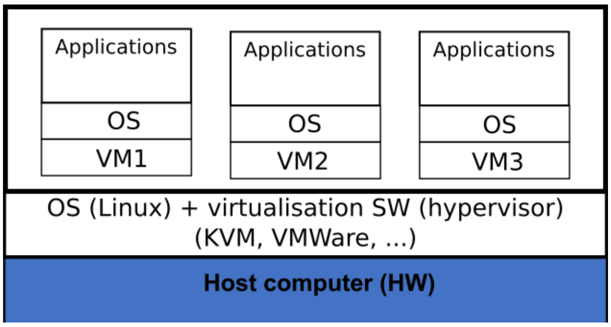

Figure 5. Architecture of the host with virtual machines.

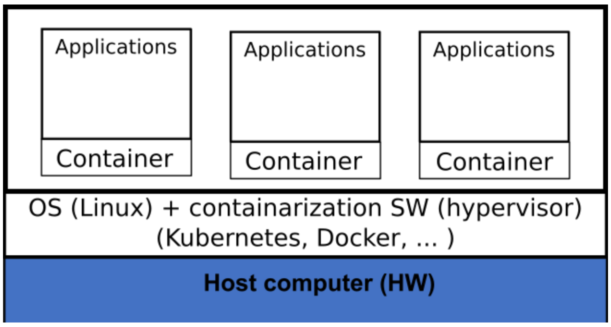

Figure 6. Architecture of the host with containerization.

users. The configuration can change – virtual computers can be added, memory, processor capacity and allocated storage capacity can be increased/decreased to individual users (customers) according to their needs. In the case of private cloud, hardware is dedicated only for one customer, infrastructure is separated and usually communicates under virtual private network. So, computation capacity and other resources are dedicated to one user (customer) and can't be provided to other users. Moreover, other safety precaution are applied like physical separation from other physical computational systems etc. It is clear that only possible variant to implement interlocking system is to use private cloud to ensure RAMS and security parameters. The most suitable operating system is Linux (it is more stable, reliable and more powerfull than MS Windows). There are several virtualization software:

- VMWare – available under Linux and Windows, in free and commercial version
- Oracle Virtual Box – available under Linux and Windows, in free and commercial version
- Hyper V – from Microsoft, only under MS Windows
- KVM – Kernel-based Virtual Machine – under Linux

System KVM is most used under Linux today. Each virtual machine has its own configuration – it has assigned some amount of physical memory, counts of processor cores, virtual network adapters assigned to physical card, virtual disks. Virtual disks can be represented (emulated) by files stored on physical storage of host computers, but it is better to use more sophisticated technologies for disk management like LVM (Logical Volume Management), ZFS (ZettaByte File System), CEPH, DRBD (Distributed Replicated Block Device). These virtualization software makes possible full virtualization: several instances of virtualization software allow to run independent instances of operating system and this system can be different from the operating system on the host computer (Linux installed in VM which runs under MS Windows and vice versa). We can even emulate other computers based on different processor (remember emulators of 8-bit computers like ZS Spectrum, Atari, Commodore on PC under MS Windows). On the other hand, the second approach is a *containerization*. It can be said that this approach is a "light" virtualization. The containerization software is represented by open-sources systems like Kubernetes, Docker. There is only one instance of operation system on host and applications run in a virtual environment – in a "package" called container (Figure 6). All virtual instances share one operating system; application must be compiled under the same operating system, i.e. it is not possible to run application for MS Windows in the containerization software running under Linux.

2.3. Virtualization and fulfilment of EN 50126, EN 50128, EN 50129

2.3.1. EN 50126 and EN 50129

The designer must fulfill a prove RAMS according to EN 50126. Thank to the virtual architecture (hypervisors) the cloud system allows a fast and automatic recovery process of HW and SW resources so that a detected failure does not compromise the function and safety of the whole system (ballancing). So, the

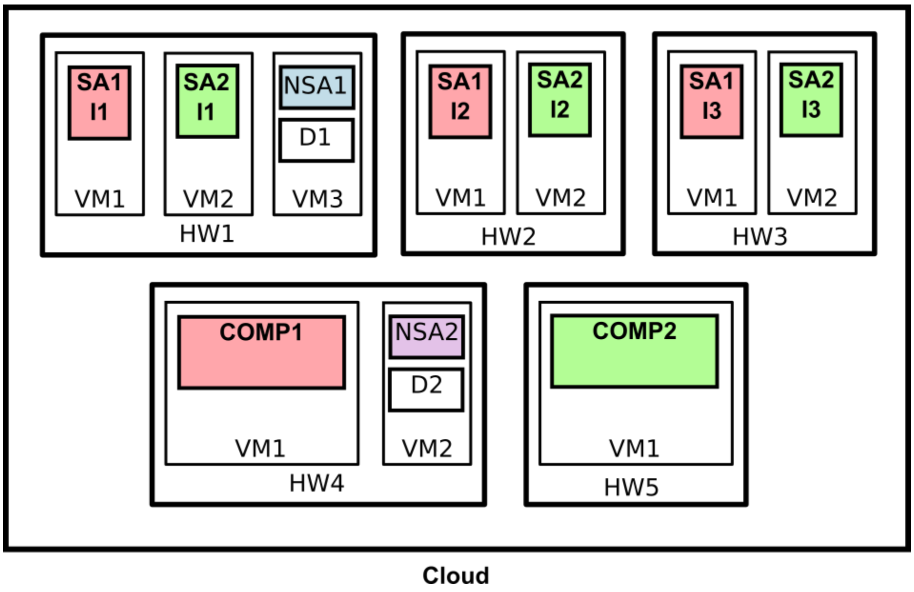

Figure 7. Example of application distribution over cloud.

reliability can be increased, but analyses of the reliability of the cloud system can be more difficult because failures with common cause have to be considered (failures of hypervisor for example). To increase the reliability the redundancy of the cloud (hot or cold stand-by) is recommended. Due to centralization accessibility and maintainability is higher than in the case of distributed system.

One parameter which influences the *safety* is an architecture of the system. The architecture is recommended in EN 50129 like an architecture M of N. As a minimum architecture, 2 of 3 is assumed to allow fail-safe operation for security integrity (SIL) at up to level 4. In the architecture 2 of 3, HW and SW must be implemented in independent instances and the results of the computation are compared. So, there must be created such configuration of the hypervisor which ensures that safety related application and comparators run in several (three in minimal) instances in separated virtual machines on separate hardware. Thank to high computational capacity of the cloud and relatively low computational demands of railway applications, there can be executed several applications (PZZ, TZZ, SZZ, ...) in one virtual machine in parallel. The example how applications can be distributed over the cloud is in the Figure 7. Two safety applications (SA1, SA2) run in three instances (SA1-I1, SA1-I2, SA1-I3, SA2-I1, SA2-I2, SA2-I3) in separate HW. Each instance has own virtual machine. The architecture is 2 of 3, COMP1 and COMP2 are comparators atteched to SA1 and SA2. Non safety applications NSA1, NSA2 and diagnostics modules D1, D2 run each only in one instance (at Basic Integrity Level). Because of the high computational capacity, tens intances of safety appplication can run in one HW node in the real Integral Interlocking System.

2.3.2. EN 50128

The fulfilment of EN 50128 criteria is not a potential problem. Application software running in virtual machines “does not see” its virtual machine, there is no difference if the software is developed for real target platform or virtual computers. So, the lifecycle, techniques, processes can be the same when the software is developed for dedicated hardware. The virtualization can help to fulfill some criteria, for example 7.3.4.9 *“Where the software consists of components of different safety integrity levels then all of the software components shall be treated as belonging to the highest of these levels unless there is evidence of independence between the higher software safety integrity level components and lower software safety integrity level components. This evidence shall be recorded in the Software Architecture Specification.”* If parts of software on different safety integrity level run in separated virtual machines it can be considered to be isolated and independend. When the software is tested it must be focused on load testing, due to sharing physical hardware.

3. Conclusions

The development of interlocking systems leads to integral interlocking system when all parts (station interlocking system, line interlocking system, level crossing interlocking systems, radio block control panel etc.) and logic is concentrated in one computational node. The approach can decrease cost for infrastructure because components are reduced to object controllers and communication lines. The central computational node can be realized by cloud – some manufacturers have already produced and deployed such solution. The implementation of interlocking system must satisfy CENELEC European standard EN 50126, EN 50128, EN 50129 and security requirements which are now in proposal. Thank to features of the cloud (centralization, stand-by, fail-safe, automatic reconfiguration, . . .), RAM parameters (Reliability, Accessibility, Maintainability) can be improved in comparison with distributed solution. It is recommended to use private cloud than public one. The attention must be given to the configuration to satisfy requirements for HW/SW architecture related to appropriate safety integrity level (for example for 2 of 3 architecture: more instances of safety related application must be executed on separate HW – even in case of reconfiguration (migrate the application to another node) after the failure).

References

[1] M. Leso. The railway 4.0 concept – the vision of a digital railway in the Czech Republic (CR). *Acta Polytechnica CTU Proceedings* **35**:27–36, 2022. https://doi.org/10.14311/APP.2022.35.0027

[2] Thales. Öbb-infrastruktur and thales work on cloud-interlocking. 2023, [2023-03-16], https://www.thalesgroup.com/en/austria/news/obb-infrastruktur-and-thales-work-cloud-interlocking.

[3] Siemens. Interlocking systems. 2023, [2023-03-16], https://www.mobility.siemens.com/global/en/portfolio/rail/automation/interlocking-systems.html.

[4] Siemens. Bane NOR and Siemens mobility celebrate milestone in digitalization of Norway's rail network. 2023, [2023-03-16], https://press.siemens.com/global/en/pressrelease/bane-nor-and-siemens-mobility-celebrate-milestone-digitalization-norways-rail-network.

[5] S. Steffens, W. Valvoda. The development of new DS3 safety platform – from the research to commissioning. *Signal+Draht* **113**(6):52–59, 2021.

[6] R. Hametner, P. Tummeltshammer, S. Resch, W. Wernhart. Cloud architecture for SIL4 railway application. *Signal+Draht* **114**(3):20–28, 2022.

[7] European standard. EN50126-1:2017. Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 1: Generic RAMS process. Standard, CENELEC, 2017.

[8] European standard. EN50126-2:2017. Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 2: Systems approach to safety. Standard, CENELEC, 2017.

[9] European standard. EN50128:2011. Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems. Standard, CENELEC, 2011.

[10] European standard. EN50129:2018. Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling. Standard, CENELEC, 2018.

[11] D. Nenutil. Kybernetická bezpečnost pro drážní systémy. *Vědeckotechnický sborník ČD* **47**:1–23, 2019.