http://dx.doi.org/10.25673/111745

A Communication Concept Using 5G for the Automated Driving Monorail Vehicle MONOCAB

Andre Bröring[1] Arne Neumann[2] Andreas Schmelter[3] Jürgen Jasperneite[4]

Abstract:

The MONOCAB is an innovative monorail vehicle designed to operate in two directions simultaneously on a single rail track. To ensure smooth operations and efficient fleet management, various communication needs arise. This paper outlines four common use cases and identifies nine communication requirements for the MONOCAB. Based on this, it presents a communication concept utilizing 5G technology, covering Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, as well as time critical communication to an edge application in a central control centre and non-time critical communication for fleet management and provision of information for the MONOCAB users.

Keywords: 5G Communication; Railway; V2X; Remote Control; Security

1 Introduction

Increasing the attractiveness of rural areas depends to a large extent on accessible mobility services and the associated connections to surrounding regions. In addition to usability and thus acceptance, a requirement for these services is cost-effectiveness. This essentially depends on the market introduction costs and the subsequent operating and maintenance costs, especially for personnel and expensive infrastructure. These factors can be kept low by reusing existing infrastructures and reducing operating costs [Fl20].

The MONOCAB, shown in Figure 1, is an automated driving monorail vehicle that can drive on a single rail track with several vehicles simultaneously in two directions, enabling a bidirectional on-demand mobility service [GMS21]. The prerequisite for such an automated driving vehicle are suitable technological measures, which require reliable internal and external communication mechanisms. In order to avoid heavy investments in rebuilding the traditional rail communication systems used by trains with signal lights, railway crossing gates and sensors, and sensors for rail clearance signals, a proprietary communication system should be used. This should enable the communication between the MONOCABs and a central control centre, as well as between individual MONOCABs and between the MONOCABs and the infrastructure, for example at railroad crossings. Such a communication system must comply with time barriers in transmission time, allow sufficient bandwidth,

---

[1] Institute Industrial IT - inIT, Campusallee 6, 32657 Lemgo, Germany, andre.broering@th-owl.de

[2] Institute Industrial IT - inIT, Campusallee 6, 32657 Lemgo, Germany, arne.neumann@th-owl.de

[3] Institute Industrial IT - inIT, Campusallee 6, 32657 Lemgo, Germany, andreas.schmelter@th-owl.de

[4] Fraunhofer IOSB-INA, Campusallee 1, 32657 Lemgo, Germany, juergen.jasperneite@iosb-ina.fraunhofer.de

Fig. 1: Photo of the MONOCAB Demonstrator named 'Thusnelda' in 2023

e.g. for video streams of the MONOCAB surroundings, and be robust against (wilful) disturbances.

This paper presents a corresponding communication concept based on the 5G communication standard. Section 2 describes the typical use cases and requirements for the MONOCAB communication. Based on that, Section 3 gives an overview of available technologies for the required communication system, leading to the communication concept in Section 4.

2 Use Cases and Requirements

2.1 Use Cases

In driving operation, situations, such as preceding, following, and oncoming MONOCABs, typical infrastructure along the track, as well as malfunctions of the vehicle itself are relevant. This minimum selection of driving situations results in the external communication interfaces, which are briefly described by four Use Cases for the communication system:

Use Case 1: As the MONOCABs pass each other close on a single track, a communication to oncoming MONOCABs in a **Vehicle-to-Vehicle (V2V)** communication can be used to exchange status information, such as position, velocity, acceleration, and vertical stabilization status. In addition, the V2V communication can support the object identification by sharing sensor data for environmental perception of objects along the rail track. For following MONOCABs, the communication can enable a closer distance by the synchronization of the velocity and acceleration, similar to the platooning of road trucks during collaborative cruise control [TJS16]. The data exchanged can complement the local sensor data of each MONOCAB for an enhanced vertical stabilization control and driving operation. This requires very low latencies to enable an appropriate reaction to new data.

Use Case 2: The **Vehicle-to-Infrastructure (V2I)** communication, for the connection to the infrastructure, such as railroad crossings of MONOCAB tracks and roads, can optimize the coordination of MONOCABs and road traffic. A communication to connected cars can even enhance the coordination. Sensor data from infrastructure systems in occupied sections can be exchanged for the environmental perception of objects and provide environmental data, such as wind, rainfall, and temperature, to adapt the MONOCAB driving operation, for example by a reduced driving speed.

Use Case 3: In case of emergencies or obstacles on the rail track that can not be identified by the system enabling the automated driving, a human operator can take over the control and move the MONOCAB out of the unclear situation via **remote control from an external control centre**. Therefore, the transmission of remote control commands as well as video streams of the MONOCABs surroundings and inside are required. This necessitates a low latency and high uplink data rate from the MONOCAB in a one-to-one communication between MONOCAB and control centre. As an assumption, the speed during the remote control is limited to 6 km/h to enable a safe breaking distance.

Use Case 4: In addition to the remote control from the control centre, less time-critical data for a **MONOCAB fleet management**, such as the battery status, has to be transferred continuously from all MONOCABs to the control centre. In the other direction, the control centre distributes information with the next stop and driving job for each MONOCAB. This communication requires a continuous communication between many MONOCABs and a single endpoint in a bidirectional many-to-one communication.

According to the four described use cases, the communication demands and capabilities of a MONOCAB can be contextualized close to the automotive domain, which puts many efforts into similar functionalities, such as teleoperated driving and V2X communication. On the other hand, technologies from the railway domain could be relevant, as the MONOCAB is operated on a rail track and has less possible driving manoeuvres compared to a road vehicle, as it is bound to the rail track. Nevertheless, the railway domain has different requirements for the typical much larger and faster trains. In addition, the railway technologies have to be compatible with the legacy communication systems on the existing rail tracks simultaneously used by accompanying trains. For the MONOCAB, a concept with an independent proprietary communication system will be proposed here.

2.2 Requirements

As mentioned in the Use Cases, a low latency for the direct control via remote control is needed. In addition to the communication system latency, video encoding and decoding, application latencies on MONOCAB and control centre side, as well as the reaction time of the operator have an impact on the total service latency for the remote control operation. In a study, the latency of the communication system is assumed with only one third of the total end-to-end service latency [5G21].

In the railway domain, a study assumes a total roundtrip latency for the communication system including the transmission of the video streams and control signals of 20 ms for a train remote control below 40 km/h [Ce21]. In the automotive domain, different projects identified different maximum latency values for teleoperated driving. In one project, the total latency of the communication system is assumed to be 60 ms for driving slower than 50 km/h [5G21]. As the MONOCAB is much smaller and lighter than a train and driving only 6 km/h in a remote control situation, we adapt the values from the automotive domain. This results in a latency of 60 ms roundtrip time for the communication system during remote control operation (**REQ.01**).

In addition to the low latency during the remote control, there is high data throughput needed. The uplink data throughput from a MONOCAB is expected with about 33 MB/s (**REQ.02**). This consists of four high definition video streams for the MONOCAB surroundings and inside, each using 8 MB/s. The control commands, status information and potential audio signals can be expected with less than 1 MB/s [5G21].

For the V2V communication in a platooning scenario, a service level latency of 50 ms is required in the automotive domain [5G23] and adapted for the MONOCAB (**REQ.03**). The V2V communication should be possible for a MONOCAB speed up to 80 km/h, resulting in a relative speed of 160 km/h (approx. 44 m/s) for oncoming MONOCABs (**REQ.04**). The resulting minimum range depends on the breaking distance of the MONOCAB as well as the time to establish a V2V communication. As both values are currently unknown, testes with the MONOCAB and a V2V communication system are pending. For now, a V2V communication distance of 440 meters (**REQ.05**) is assumed to enable a communication between two oncoming MONOCABs within 10 seconds at maximum speed.

Another important topic are different demands on service quality in terms of latency and data rate while communicating to multiple endpoints simultaneously. As a result, there is a prioritization of certain communication relations needed, for example with a higher priority for the remote control situations and safety relevant communication (**REQ.06**).

During all the use cases and scenarios, interference with private communication devices along the MONOCAB track and of MONOCAB passengers should be avoided (**REQ.07**). The MONOCAB is only used in a very limited area of reactivated disused tracks (**REQ.08**).

With regard to ICT (Information and Communication Technology) security of the MONOCAB, it is necessary to create security that is independent of other communication participants, or to establish a base-line security that works in every network without further latencies due to additional data processing for encryption and signatures (**REQ.09**). In the context of the objectives of the MONOCAB, the authenticity and integrity of the data and, depending on the data type, the confidentiality must be in the foreground of such a solution, depending on the type of data transmitted and the resulting need for protection. On the one hand, driving commands are transmitted from the control centre to the vehicle during the remote control. Secrecy is unnecessary here, but the protection of authenticity and integrity is. The same applies to the transmitted data for the MONOCAB fleet management. The situation is different with regard to any audio and image transmissions from the interior of the vehicle. These must additionally be protected with regard to their confidentiality.

3 State of the Art

5G is the first generation of mobile networks enabling the realization of stand-alone, standard-based private wireless networks in addition to public land mobile networks [Ro19] in order to support a broad range of vertical industries including mobility. These private networks can be implemented in a separate network infrastructure as well as an isolated virtual 5G network slice of a public infrastructure [5G19].

In [He22] the future 5G for railways (5G-R) was introduced, that in comparison to 5G shows some advantages, such as a higher reliability and handover success rate. Nevertheless, V2V communication is not part of the development. The end-to-end latency tends to be higher and the data rate tends to be smaller for 5G-R compared to 5G [He22]. The focus of 5G-R is the integration into the existing complex and diverse railway applications that have different requirements compared to the MONOCAB. Since traditional train control systems, such as the European Train Control System (ETCS), are not relevant for the MONOCAB operation, a proprietary system should be used that enables the usage of a rail track only with MONOCABs. As a result, normative standards and solutions targeting the high demands for railway systems with high-speed railways and large wagon trains are out of scope here.

In the automotive domain, scenarios and use cases similar to the use cases described for the MONOCAB are currently under development. According to the roadmap of the 5GAA (5G Automotive Association) for C-V2X (Cellular-V2X), automated driving, including automated parking and teleoperated driving similar to remote control for the MONOCAB, are possible in local areas and campuses using 4G. A transition to 5G-based communication is started. The sharing of dynamic objects, sensor signals, complex interactions, and cooperative manoeuvres are in development [5G22]. As mentioned before, the technologies used for the automotive domain are taken into account for the MONOCAB communication system due to similarities in the use cases and requirements.

For the V2X communication, there are two main solutions available and under development. C-V2X is part of the 3rd Generation Partnership Project (3GPP) standards. A direct communication via LTE-V2X was introduced in 3GPP Release 14 using the PC5 interface. The following 3GPP releases up to Release 17 bring up enhancements for the C-V2X communication, such as a latency of about 1 ms and a transition from LTE-V2X to 5G-V2X [MVH21]. The other standard for the V2X communication is based on IEEE

802.11p, using a WLAN-based direct communication. The enhanced standard 802.11bd is in development [MVH21, NCP19]. A comparison of the two standards from the 3GPP and IEEE leads to advantages and greater support of the C-V2X communication. It has benefits, such as longer communication distances, an integration into existing cellular infrastructure, and the support of the 5GAA [5G16] presumably leading to a wide adoption in the automotive domain.

With regard to ICT security, 5G has been significantly further developed compared to previous mobile radio standards. On the part of standardisation, security is specified, starting with security management through network monitoring systems to the classic protection goals of confidentiality, integrity, and authenticity. A challenge for ICT security in 5G networks lies in the inhomogeneity between network operators and the multitude of user equipment (UEs) involved. A study commissioned by the European Union [NI20a] shows potential vulnerabilities in the 5G network, which are located both in possible misconfigurations, but also in the confluence of the most diverse device manufacturers and network providers with different implementations. Overall, it can be seen that the security features of 5G standardisation are fine, but their implementation and thus use are often optional and thus dependent on the device manufacturer and mobile network provider [NI20a, para. 3.3]. A more general overview on IT-Security issues, based on the basic technologies used in 5G, is given by [Ah17].

Similar to the developments of the 3GPP C-V2X standard, the 3GPP Release 16 and Release 17 introduce new general features for 5G useful for the presented MONOCAB Use Cases. This includes the support of ultra reliable low latency communication (uRLLC) [Fo21]. Up to now, most hardware that is currently available only supports 3GPP Release 15 [Ha23]. Hence, a realization of the presented features is not possible at the time of writing this paper.

4 Communication Concept

Based on the state of the art, the use cases, and requirements, a concept for the MONOCAB communication is developed. The overall communication is shown in Figure 2. Here, network transitions to the Controller Area Network (CAN) protocol integrate the MONOCABs control units while all other end devices utilize IP based protocols.

4.1 Communication to Control Centre

In order to be independent of network operators and to limit the interference of the MONOCAB communication with the communication of passengers as well as other users of the public 5G network along the track (**REQ.07**), the MONOCAB communication system is based on a standalone NPN. Therefore, the MONOCAB communication can operate in a 5G network using a licensed private frequency for the limited area around the MONOCAB

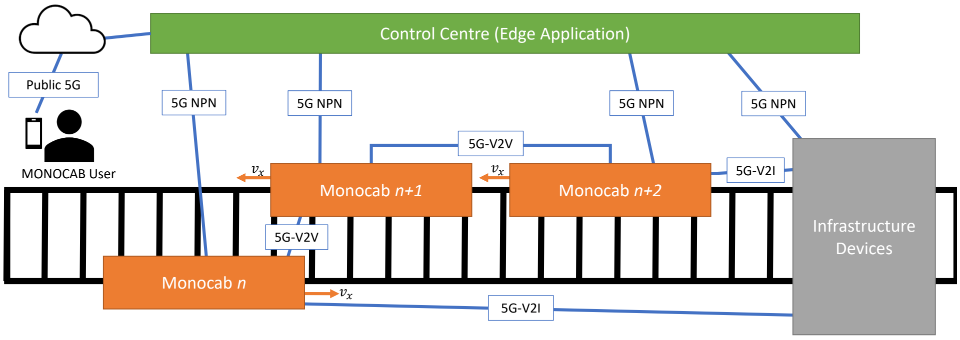

Fig. 2: Communication of three MONOCABs, the Control Centre, Infrastructure, and User

rail track (**REQ.08**). To make the system more resilient, e.g. in case of a network failure of the standalone NPN, the public network can act as a backup solution.

The solution based on an NPN also enables to run the MONOCAB control centre as an edge application. This can reduce the latency and increase the Quality of Service (QoS) [HYW19], especially for the remote control (**Use Case 3**). In a 5G outdoor field test with one MONOCAB, the added latency when using a 5G communication compared to a wired communication was about 26 ms from 119 ms (wired) to 145 ms (with 5G) glass-to-glass video stream service latency [Gu23]. However, more extensive practical tests to measure the latency (**REQ.01**) and data throughput (**REQ.02**) of a remote control application when operating a whole fleet of MONOCABs in a 5G network are pending.

The monitoring and management of the MONOCABs and the infrastructure can be realized as an edge application as well. The control centre can collect data, e.g. about the status of railroad crossings, from the infrastructure facilities. This non-time critical data can be transferred to and managed in a cloud service. From the cloud service, selected data can be made available for the MONOCAB users. To separate the different time-critical and non-time-critical communication, different slices or QoS profiles can be used for remote control (**Use Case 3**) and fleet management (**Use Case 4**) to fulfil **REQ.06**.

4.2 V2X Communication

The 5G-V2X or IEEE 802.11p based communication can be used to realise **Use Case 1** and **Use Case 2**. The advantage of the integration into the planned 5G communication infrastructure for the MONOCAB leads to a recommendation to adopt the 5G-V2X standard. An additional benefit is the support of the 5GAA [5G16], enabling a compatibility with the road traffic without multiple hardware and enabling the integration of road traffic and road safety messages, as well as pedestrian and bicycle protection as a part of 5G-V2X [5G22] into the MONOCAB communication.

A 4G-based V2V latency test using the PC5 interface resulted in a latency around 30 ms, hence lower than the 100 ms defined in the 3GPP Release 14 [MVH21] and fulfilling **REQ.03**. Another advantage of the C-V2X standards in comparison to IEEE 802.11p is a low end-to-end delay for longer distances. According to a simulation, a communication of safety broadcast messages could be realized with the C-V2X solution between two vehicles over a distance greater than 525 m with a delay of 4.2 ms, outperforming the simulation results when using IEEE 802.11p [Th18]. The distance is also fulfilling **REQ.05**. Newer systems following newer releases aim to further decrease the latencies. In another simulation, the V2X sidelink communication in the mmWave-band was independent of the vehicle velocity up to 300 km/h [Ki21], hence fulfilling **REQ.04**. However, the range in the higher frequency bands (mmWave-band) is limited and was out of scope in the simulations [Ki21]. Tests and simulations for the V2X communication with different velocities in the Sub-6-GHz frequency bands with a higher range are pending.

In addition to the infrastructure monitoring via the proposed edge application in the control centre, data can be exchanged directly between a MONOCAB and close infrastructure devices, for example at railroad crossings, using C-V2I communication (**Use Case 2**) similar to the C-V2V communication.

4.3 ICT Security

Each of the identified protection goals in **REQ.09** requires cryptographic procedures, such as encryption and signatures, which use different algorithms. The New Radio Integrity Algorithm (NIA) and New Radio Encryption Algorithm (NEA) procedures, which are AES-based and offer good protection, are primarily to be used [Co22]. A particular challenge arises from the combination of the required low latencies and cryptographic protocols and their partly non-deterministic computing time, for example for key generation, data encryption and decryption. These must not be violated under any circumstances. Established procedures, such as IPsec, come into consideration here [NI20b]. What is promising about these protocols is that they create end-to-end security, which is also demanded or recommended in other scientific works [Ku18, Zh22, Ah17].

5 Conclusions and Outlook

The concept presented in this publication shows to what extent the current mobile radio standard 5G can be used in the example of the automated driving monorail vehicle MONOCAB in theory. The criteria for this were developed on the basis of selected use cases and requirements. A concept covering the use cases and requirements is presented based on the state of the art in the 5G technology. Due to missing hardware supporting the needed functionalities of the recent 5G standards, practical implementations and tests for the whole concept are pending in order to prove the fulfilment of all presented requirements.

First experiments for a 5G-based MONOCAB communication were already executed and documented in [Gu23]. Nevertheless, more measurements with future hardware supporting the newer 3GPP Releases should be executed, especially in the environment of a rail tracks in rural areas that can be used by MONOCABs. The resulting characteristics of the 5G communication and the influence on the mentioned use cases can be analysed to further improve the concept.

Acknowledgement

This work was funded by the Ministry of Economic Affairs, Innovation, Digitalization, and Energy of the State of North Rhine-Westphalia in the research project “5G SIMONE - sicher.mobil.vernetzt.”

Bibliography

[5G16] 5GAA Automotive Association: The Case for Cellular V2X for Safety and Cooperative Driving. White Paper, 2016.

[5G19] 5G-ACIA: 5G for Automation in Industry. White Paper, 2019.

[5G21] 5GAA Automotive Association: Tele-operated Driving (ToD): System Requirements Analysis and Architectures. Technical Report, 2021.

[5G22] 5GAA Automotive Association: A visionary roadmap for advanced driving use cases, connectivity technologies, and radio spectrum needs. White Paper, 2022.

[5G23] 5GAA Automotive Association: C-V2X Use Cases and Service Level Requirements Volume II. Technical Report, 2023.

[Ah17] Ahmad, Ijaz; Kumar, Tanesh; Liyanage, Madhusanka; Okwuibe, Jude; Ylianttila, Mika; Gurtov, Andrei: 5G security: Analysis of threats and solutions. In: 2017 IEEE Conference on Standards for Communications and Networking (CSCN). pp. 193–199, 2017.

[Ce21] Cellarius, Bastian; Fritzsche, Richard; Lohmar, Thorsten; Kuo, Fang-Chun: Design of an FRMCS 5G E2E System for Future Rail Operation. Study Report, 2021.

[Co22] Cowperthwaite, Alex: A 5G Security Overview: Features, Rewards, and Risks of 5G Technology. KROLL, 2022.

[Fl20] Flasskamp, Martin et. al.: Vorstudie vernetzte Mobilität OWL. Ministerirum für Verkehr des Landes NRW, 2020.

[Fo21] Fodor, Gábor; Vinogradova, Julia; Hammarberg, Peter; Nagalapur, Keerthi Kumar; Qi, Zhiqiang Tyler; Do, Hieu; Blasco, Ricardo; Baig, Mirza Uzair: 5G new radio for automotive, rail, and air transport. IEEE Communications Magazine, 59(7):22–28, 2021.

[GMS21] Griese, Martin; Mousavi, Seyed Davood; Schulte, Thomas: Modeling the vertical dynamics of a self-stabilizing monorail vehicle. In: 2021 9th International Conference on Control, Mechatronics and Automation (ICCMA). IEEE, pp. 205–210, 2021.

[Gu23] Gustin, Denis; Siekmann, Timo; Kroll, Björn; Kleen, Philip; Schriegel, Sebastian; Jasperneite, Jürgen: Outdoor Field Test of 5G-based V2X Communication for Real-Time Monitoring and Remote Control of a Monorail Vehicle. In: 2023 IEEE 21st International Conference on Industrial Informatics (INDIN). IEEE, pp. 1–6, 2023.

[Ha23] Hardesty, Linda: Chips are holding back 5G private wireless. `https://www.fiercewireless.com/private-wireless/private-network-use-cases-expand-verizon`, 2023. Accessed: 2023-09-05.

[He22] He, Ruisi; Ai, Bo; Zhong, Zhangdui; Yang, Mi; Chen, Ruifeng; Ding, Jianwen; Ma, Zhangfeng; Sun, Guiqi; Liu, Changzhu: 5G for Railways: Next Generation Railway Dedicated Communications. IEEE Communications Magazine, 60(12):130–136, 2022.

[HYW19] Hassan, Najmul; Yau, Kok-Lim Alvin; Wu, Celimuge: Edge computing in 5G: A review. IEEE Access, 7:127276–127289, 2019.

[Ki21] Kim, Junhyeong; Noh, Gosan; Kim, Taehyoung; Chung, Heesang; Kim, Ilgyu: Link-level performance evaluation of mmwave 5g nr sidelink communications. In: 2021 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, pp. 1482–1485, 2021.

[Ku18] Kumari, K. Anitha; Sadasivam, G. Sudha; Gowri, S. Shymala; Akash, Sebastin Arockia; Radhika, E.G.: An Approach for End-to-End (E2E) Security of 5G Applications. In: 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS). pp. 133–138, 2018.

[MVH21] Miao, Lili; Virtusio, John Jethro; Hua, Kai-Lung: PC5-based cellular-V2X evolution and deployment. Sensors, 21(3):843, 2021.

[NCP19] Naik, Gaurang; Choudhury, Biplav; Park, Jung-Min: IEEE 802.11 bd & 5G NR V2X: Evolution of radio access technologies for V2X communications. IEEE access, 7:70169–70184, 2019.

[NI20a] NIS Cooperation Group: Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. `https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures`, 2020.

[NI20b] NIS Cooperation Group: A Guide to 5G network security 2.0. `https://www.ericsson.com/en/security/a-guide-to-5g-network-security`, 2020.

[Ro19] Rostami, Ahmad: Private 5G Networks for Vertical Industries: Deployment and Operation Models. In: 2019 IEEE 2nd 5G World Forum (5GWF). pp. 433–439, 2019.

[Th18] Thota, Jayashree; Abdullah, Nor Fadzilah; Doufexi, Angela; Armour, Simon: Performance of car to car safety broadcast using cellular V2V and IEEE 802.11 P. In: 2018 IEEE 87th Vehicular Technology Conference (VTC Spring). IEEE, pp. 1–5, 2018.

[TJS16] Tsugawa, Sadayuki; Jeschke, Sabina; Shladover, Steven E: A review of truck platooning projects for energy savings. IEEE Transactions on Intelligent Vehicles, 1(1):68–77, 2016.

[Zh22] Zhao, Jinghao; Li, Qianru; Yuan, Zengwen; Zhang, Zhehui; Lu, Songwu: 5G Messaging: System Insecurity and Defenses. In: 2022 IEEE Conference on Communications and Network Security (CNS). pp. 37–45, 2022.