Q1/2026

WHITE PAPER

WIRELESS SAFETY FOR AMR CONTROL

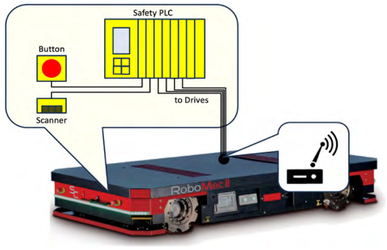
R3 Solutions

A Peppermint Company

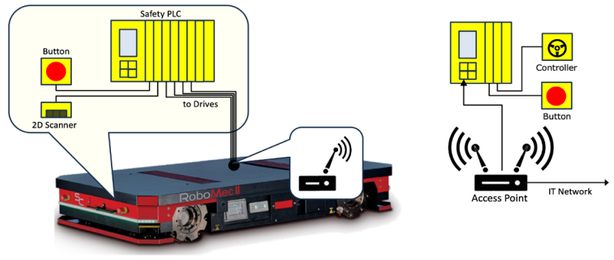
R3 Solutions GmbH Kurfürstendamm 194 · 10707 Berlin · Germany · contact@r3.group · www.r3.group

WHY AMRS NEED WIRELESS SAFETY

Autonomous Mobile Robots (AMRs) must comply with stringent functional safety requirements. To achieve this, they are equipped with onboard safety, that means that the safety functions necessary for safe operation are fully integrated within the robot itself, rather than relying on external safety systems. In practice, this includes components and capabilities such as safety sensors (e.g., LiDAR scanners, cameras, and bumpers) that enable reliable detection of obstacles and personnel in the robot's environment.



AMR with onboard safety and Wi-Fi client.



AMR with combined onboard & wireless safety over Wi-Fi client.

Failsafe over EtherCAT represents a special case in wireless environments. FSoE / FSWE can operate using two communication models: the EtherCAT Device Protocol, which is highly deterministic and requires microsecond-level synchronization—well suited for wired systems but challenging in wireless contexts—and the EtherCAT Application Protocol, which enables master-to-master communication with lower synchronization requirements, making it more suitable for wireless use.

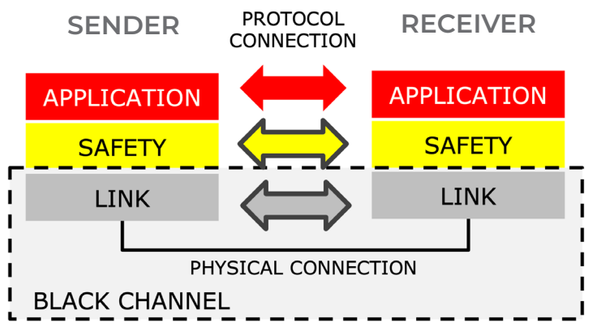
For communication with their environment, most AMRs are equipped with a Wi-Fi client or industrial PCs (iPCs) featuring a Wi-Fi network interface card (NIC). Thanks to their self-contained safety architecture, AMRs are able to navigate safely in dynamic environments, detect hazards, and respond immediately—by stopping, slowing down, or rerouting—even in the event of a network outage, until connectivity is restored.

So why is WIRELESS SAFETY for AMRs considered important? There are several compelling reasons, with the top three being:

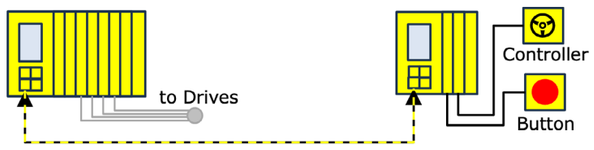
1. Limitations for human–robot interaction: Onboard safety systems might not be strong enough for efficient and flexible interaction between humans and robots.
2. Limitations for robot-machine interaction: Onboard safety systems can limit interaction by preventing intended or necessary proximity.
3. Requirement for wireless emergency stop: Regulatory frameworks, such as Regulation (EU) 2023/1230 on machinery (LINK), require remote supervisory and emergency stop capabilities.

BLACK CHANNEL PRINCIPLE

Safety protocols were originally designed for stable, deterministic, cable-based networks—not for inherently unstable wireless environments such as Wi-Fi. Nevertheless, they can be applied to Wi-Fi through the BLACK CHANNEL approach. In this model, the communication network is treated as unknown and potentially unreliable, while safety is ensured entirely at the protocol level. In simple terms, the safety protocol introduces a safety layer between the application and the underlying communication link, whose primary role is to verify that the connection is active and that data can be transmitted reliably. To achieve this, the safety layer on the sender side periodically transmits a safety probe message to the receiver, effectively asking, "Are you reachable?" Upon receiving this message, the safety layer on the receiver side immediately responds with a corresponding safety message confirming, "Yes, I am."



The safety layer guarantees safe operation over an unknown link.



Remote safety application using an Ethernet Safety Protocol via cable.

Whenever a safety packet is lost or delayed beyond acceptable limits, the system automatically transitions into a fail-safe state. Given that Wi-Fi networks, by their nature, are prone to packet loss and latency variations, this can lead to frequent and repeated activations of the FAIL-SAFE MODE.

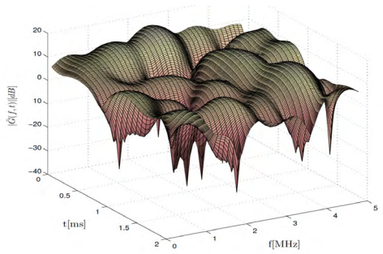
ETHERNET-BASED SAFETY PROTOCOLS

A variety of industrial safety protocols are available, including PROFIsafe (PROFINET), CIP Safety (EtherNet/IP), CC-Link Safety, Failsafe over EtherCAT (FSoE / FSWE), SafetyNET *p* (Pilz), Safe IP / Safe Shield IP, and manufacturer-specific protocols, e.g., from BBH (among others used by Schmersal). These protocols differ fundamentally in terms of communication sequences, packet structures, timer and watchdog concepts. Proprietary approaches in particular (e.g., BBH-based protocols) demonstrate that additional, individualized process and timing models exist, which must be analyzed separately in the wireless context. The different safety protocols generate distinct traffic profiles: PROFINET / PROFIsafe operates with cyclic frames, with packet size increasing as the number of I/Os grows; CIP Safety establishes additional connections for each I/O pair, leading to higher load due to an increasing number of parallel streams; and SafetyNET p generates redundant telegrams within each cycle and incorporates additional heartbeat communication.

INTERACTION BETWEEN SAFETY PROTOCOL AND WIRELESS CHANNEL

Overall, the robustness of a wireless safety architecture is primarily determined by the choice of safety protocol, the underlying wireless technology, and the interaction between the safety protocol, network state, and wireless channel dynamics. In contrast to the relatively stable characteristics of wired connections, wireless channel quality continuously varies over time, frequency, and space.

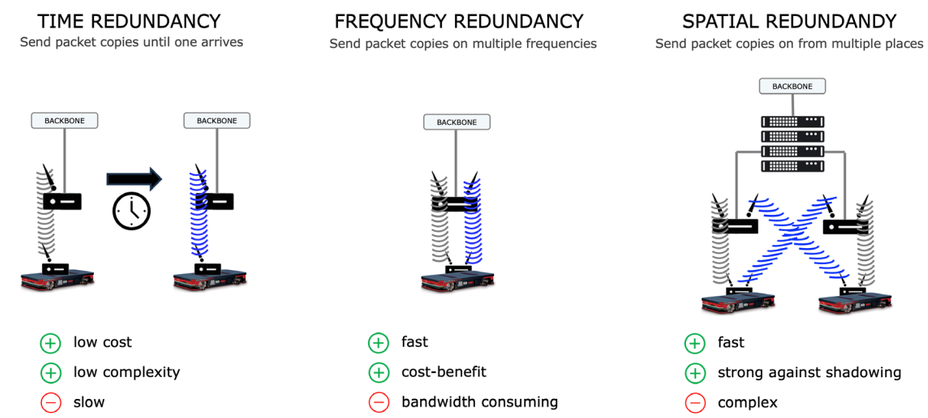
Consequently, a key requirement for the wireless system is to compensate for fluctuations in channel quality to ensure reliable transmission of safety packets. This requires consideration of the different phases of the safety protocols. The startup phase is characterized by larger packets, parallel connection setups, increased network load, and active timeouts, whereas the operational phase involves stable cyclic traffic and deterministic behavior. Notably, the startup phase is often more critical than normal operation.



Wireless channel quality *G(t)* at a given location as a function of time *t* and frequency *f*.

ACHIEVING WIRELESS NETWORK RELIABILITY

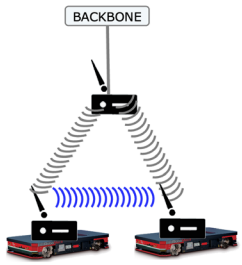
To address channel volatility and ensure stable transmission across all phases of safety protocols, packet copies are transmitted from sender to receiver using various methods, leveraging redundancy in time, frequency, and space. Standard Wi-Fi systems primarily exploit time redundancy through retransmissions of lost packets, while technologies such as Wireless IO-Link utilize frequency redundancy by transmitting packet copies in parallel on different frequencies. 5G networks, in turn, can leverage spatial redundancy by enabling coordinated multi-point transmissions (CoMP).



Packet copies can be sent after the original or in parallel via different frequencies / from different locations.

MASSIVE COOPERATION FOR RELIABLE WIRELESS NETWORKING

A specific approach to leveraging spatial redundancy in wireless channels to enhance system reliability is massive cooperation. In this concept, for each transmission, the sender selects an additional receiver—alongside the intended recipient—from a group of available nodes. In the context of AMRs, this means that another robot is designated to also receive a packet intended for a specific AMR. If the intended recipient fails to receive the packet, this additional receiver (referred to as the "*buddy*") retransmits it within microseconds. The likelihood of successful delivery is significantly increased, as the buddy is selected based on strong connectivity to both the sender and the intended receiver.



⊕ fast
⊕ strong against shadowing
⊕ cost-benefit

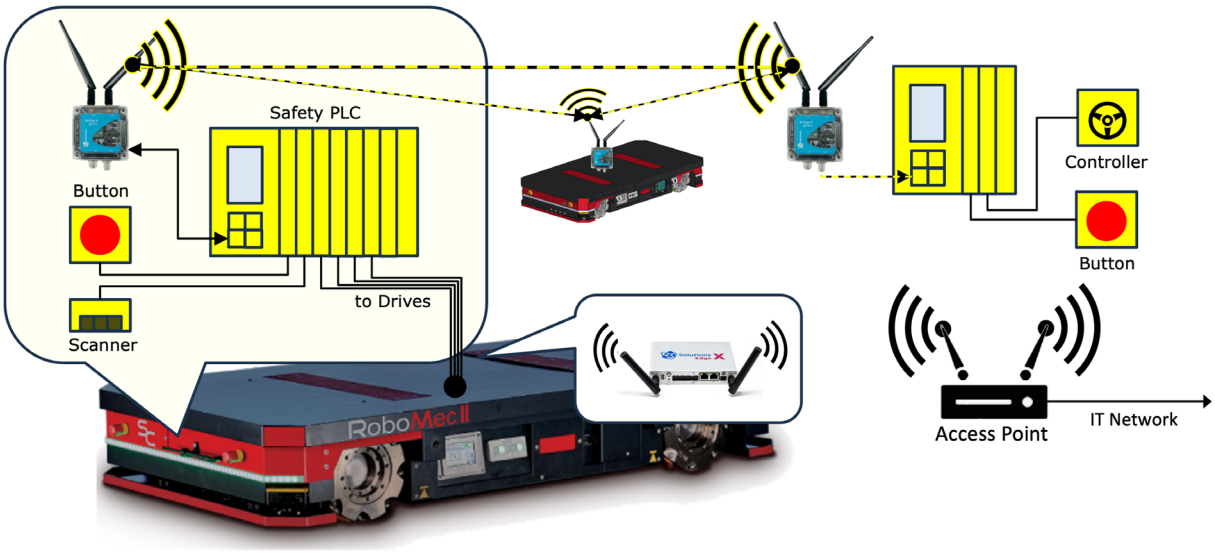
Massive cooperation mode.

ROAMING AS A CRITICAL TRANSITION

Roaming is essential to ensure seamless wireless coverage across larger areas. However, it represents a critical transition phase that can impact communication performance. During roaming, temporary communication interruptions may occur, latency can increase, and additional protocol as well as security-related overhead is introduced. At the same time, safety mechanisms such as watchdogs and timeouts continue to operate uninterrupted. This mismatch between continuous safety supervision and temporary communication degradation increases the likelihood of safety-related events, such as unintended stops or fault conditions. A key approach to mitigating this challenge is triggered roaming, for example based on the AMR's position rather than on observed signal strength.

DEDICATED WIRELESS OT OVERLAY NETWORK

Many of the challenges outlined above can be effectively addressed by implementing a dedicated wireless OT overlay network architecture. In addition to the existing Wi-Fi infrastructure, a separate wireless network is deployed that is specifically optimized for the transmission of safety protocols. Depending on the use case, this dedicated OT network can even replace the standard Wi-Fi connection on the AMR.



Example of a safety wireless overlay architecture utilizing R3's Bridge E for the transmission of safety-critical control data, alongside Edge X operating as a standard Wi-Fi client for routine data exchange between AMRs and the infrastructure. Bridge E incorporates EchoRing, R3's medium access control layer specifically designed for safety and control communication, featuring capabilities such as massive cooperation, guaranteed channel access and triggered roaming.

R3 Solutions

A Peppermint Company

With the kind permission of ServisControl s.r.o.