Towards a Reliable Parallel Redundant WLAN Black Channel

Markus Rentschler
Hirschmann Automation & Control GmbH
72654 Neckartenzlingen
Markus.Rentschler@belden.com

Per Laukemann
University of Applied Sciences Esslingen
73733 Esslingen
pelait01@hs-esslingen.de

Abstract

WLAN according to standard IEEE 802.11 is widely regarded unsuitable as communication channel for real-time and safety applications. Non-determinism and interference liability leads to packet loss, exceeded and variable latency times due to retransmissions.

This work proposes a method that compensates such consequences of stochastic channel fading by the parallel operation of diverse wireless channels, applying frequency and space diversity techniques. A fault-tolerant wireless "black channel" is achieved that is able to fulfill soft real-time availability plus providing redundancy. This is realized with standard WLAN components and the "Parallel Redundancy Protocol" (PRP) according to IEC 62439-3. Reliability and performance characteristics are derived from measurements on an experimental setup with SafetyNET p nodes.

1. Introduction

IEEE 802.11 [1] (WiFi) based networks are basically the wireless extension of the Ethernet based IEEE 802.3 Local Area Networks. Higher layer LAN protocols and internetworking protocols, like TCP/IP, integrate seamlessly in this WLAN environment.

On the other side, real-time requirements for industrial applications, such as a guaranteed maximum latency times for packet transmission, are often not reliably met in IEEE 802.11 channels. Uncontrollable radio interference leads to packet loss and excessive frame retransmissions on the nondeterministic wireless MAC layer, resulting in dropped packets or intolerably high latency on the application level.

For these reasons, WLAN according to standard IEEE 802.11 is widely regarded as an unsuitable communication channel for real-time and safety applications such as SafetyNET p [6], which was the initial problem statement that led to this work and its findings.

A lot of previous work to improve the capabilities of wireless communication systems has already been done by many researchers, e.g. [2] [3]. It is well known that the performance of such systems can be significantly improved by applying diversity concepts [4] [7] [8]. The goal with diversity is to achieve stochastically independent redundancy within a wireless communication system to significantly increase reliability and availability. Redundancy is a commonly used technique for reliability enhancement.

In this work, the "Parallel Redundancy Protocol" (PRP) [5] is applied as diversity combination method on the wired Ethernet interfaces of two independent and diverse IEEE 802.11 WLAN channels that operate in parallel on point-to-point links. It is investigated by application of SafetyNET p (RTFN) communication [6] whether this system forms a reliable *black channel* suitable for such safety applications.

The paper is structured as follows: In chapter 2 to 4, brief overviews of the underlying technologies used in this work are given. This includes the basics of wireless diversity techniques, PRP, the different 802.11 standards and SafetyNET p, which is used as measurement application. In chapter 6, the related experimental setups are described. Chapter 7 describes the performance measurements, whereas chapter 8 concludes on the results and the possible further work.

2. Wireless Diversity Techniques

The basic idea behind diversity is redundant transmission of information over uncorrelated (stochastically independent) channels that only with a small probability are erroneous at the same time window. In Brennan's classical 1959 paper [4], the following basic forms of diversity for wireless communication are described:

Space diversity: The same signal is transmitted in parallel over several different propagation paths. This can effectively combat reflections, shadowing and multi-path propagation fading.

Time diversity: The same signal is transmitted more than once, but at different time instants. This can effectively combat losses due to burst interference.

Frequency diversity: The same signal is transmitted in parallel over several frequency channels or spread over a wide frequency spectrum. This can effectively combat radio interference affecting one of the frequency bands.

Polarization diversity: The same signal is transmitted and received in parallel with different field polarization.

Further diversity techniques have since been derived from the basic ones:

Antenna diversity: The most widely used form of space diversity, where multiple antennas are used on sender and/or receiver side to achieve more reliable transmissions [7].

Transmitter diversity: With multiple transmitters, space-time-coding (STC) or space-time-frequency-coding (STFC) schemes achieve a higher diversity order [7].

Receiver diversity: Signal received by multiple receivers through multiple antennas can be combined together to improve reliability [7].

Multi-Radio diversity: A combination of some of the above diversity techniques that uses multiple radios to transmit the same signal over different independent channels with different characteristics [8][9].

2.1. Diversity and Wireless Channel Behavior

Diversity methods are usually applied on the radio frequency (RF) level of the wireless system, where wireless channel fading has the following behavioural components [10]:

- path loss because of logarithmic distance attenuation,
- large-scale fading or shadowing, often modelled as log-normal,
- small-scale or multipath fading over short periods of time, commonly modelled as Rayleigh.

Over longer periods, path loss and large-scale fading are approximately constant and can be coped with using transmit power adjustment. These components of fading are very close to being correlated across all elements of a wireless diversity array (Figure 1). Diversity is therefore specifically applied to combat small-scale fading.

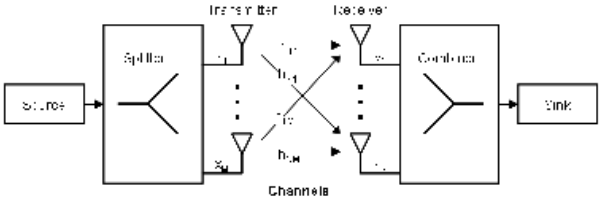

Figure 1. Diversity System with MIMO M x N channel matrix

2.2. Diversity Combining Methods

Diversity systems (see Figure 1) require a method to combine the multiple received signals into a single improved signal.

All linear diversity combiner methods are special cases of the general linear combination equation derived in [4] and can be grouped as follows:

Gain Combiner: The instantaneously received signals of all branches are added. This method requires the received signals in the same phase. Gain combining increases the *signal-to-noise-ratio* (SNR) of the overall signal at the receiver.

Selection Combiner: Only the strongest signal of all branches is selected, the other signals are ignored. This method does not increase SNR, instead it reduces the overall signal variation at the receiver.

3. Parallel Redundancy Protocol

The **Parallel Redundancy Protocol** (**PRP**) according to IEC 62439-3, Clause 4 is a static network redundancy mechanism [5]. It provides *1+1* redundancy and can therefore compensate any single network failure. It does not require network reconfiguration, providing seamless failover without affecting the data transmission with packet loss.

PRP is a layer 2 redundancy and operates independently of higher layer protocols. A PRP network consists of two different LANs with arbitrary, but similar topology. Each PRP-node has two Ethernet interfaces connected to one of the two LANs and is called a doubly attached node (DAN). Both PRP interfaces share the same MAC address. A PRP node transmits data simultaneously over the two interfaces into both networks, tagging each frame with a Redundancy Control Trailer (RTC) containing identical sequence numbers. The sequence number is incremented for each frame pair sent. The first arriving frame of a pair -identified by its sequence number- is accepted by the PRP receiver node and the second frame gets discarded. As long as one of the two LANs is operational, one frame of a pair always reaches its destination.

To use the PRP redundancy capability, non-PRP nodes must be attached through a Redundancy Box (*Red Box)*, which is a device that behaves like a DAN. A Red Box from Zurich University of Applied Sciences (zhaw) [11] and its simplified schematic is depicted in Figure 2.

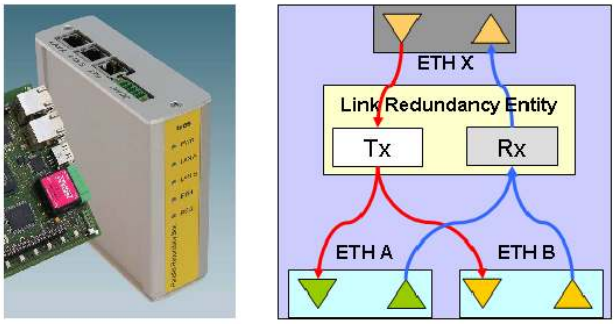

Figure 2. PRP Redundancy Box: A two-way splitter and switching combiner

Singly attached nodes (SANs) without PTP capability can also be attached to the redundant LANs, since packets without an RTC are transparently processed by the Link Redundancy Entity (LRE), which realizes the splitter and combiner functionality in a PRP node (Figure 2).

3.1. Redundancy Box as Selection Combiner

The PRP Red Box can be at the receiving side modelled as a selection combiner, where out of the two branches the "better" signal is selected, in this case the first -or faster- arriving Ethernet packet, which is then immediately further processed. The second packet -if arriving within the PRP timing window- is discarded. This can be described as follows:

$$\text{ETH X} = \begin{cases} \text{ETH A} & \text{if } (t_A < t_B) \\ \text{ETH B} & \text{otherwise} \end{cases} \quad (1)$$

t_A and t_B reflect the arrival times of a duplicated packet at the respective ETH interface.

Applying two *RedBoxes* against each other allows the creation of a diversity system with an order M = N = 2 on the Ethernet system level.

3.2. Redundancy Box Timing Behaviour

Since a four octets RCT is added to and removed from the end of the transmitted packet, the PRP splitter and combiner in a *RedBox* (see Figure 2) have both a store-and-forward behaviour with an associated delay T_{SF} = *ps/br*, where *ps* reflects the size of the transmitted packet and *br* the used bitrate. An LRE implementation-dependent delay T_{LRE} adds up to the total delay T_{RedBox} introduced by each *Redbox* in both transmission directions, expressed in

$$T_{RedBox} = T_{SF} + T_{LRE} \quad (2)$$

When the *RedBox* is realized in hardware, this delay T_{RedBox} should be similar to that of a common Ethernet switch. We have measured T_{RedBox} and computed T_{LRE} = T_{RedBox} - T_{SF} in different scenarions for the zhaw *RedBox*. Figure 3 shows the results from these measurements with different packet sizes and transmission directions at a rate of 5 packets/s. The result was that T_{LRE} is very stable below *5* µs.

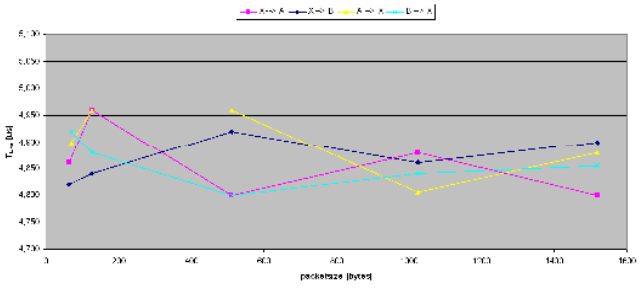

Figure 3. Measured T_{LRE} for zhaw RedBox

Another important performance criteria of the zhaw *Redbox* is the maximum processed frame size of 2000 bytes. Longer frames arriving at port ETH X will not be forwarded towards the ports ETH A and ETH B, but instead discarded by this PRP implementation.

3.3. PRP Diagnosis

Diagnosability is an important non-functional quality criteria for complex PRP networks to depict configuration and cabling errors. For this reason, some diagnosis capability has been defined for the PRP protocol in IEC 62439-3, Clause 4, Table 4. The IEC standard recommends the usage of SNMP to access the diagnostic information. The firmware version 3.3 of the zhaw *Redbox* –which was used in this experiment- however has not implemented an SNMP agent.

4. 802.11 Wireless LAN

The following IEEE 802.11 radio technologies are widely supported nowadays and offer a lot of configuration possibilities for operational diversity with *commercial-off-the-shelf* (COTS) components:

IEEE 802.11a operates in the 5 GHz band. It uses Orthogonal Frequency Division Multiplexing (OFDM) and has a maximum capacity of 54 Mbps.

IEEE 802.11b operates in the 2.4GHz band. It uses Direct Sequence Spread Spectrum Multiplexing (DSSS) and has a maximum capacity of 11 Mbps.

IEEE 802.11g operates in the 2.4GHz band. It uses OFDM or DSSS and has a maximum capacity of 54 Mbps. Table I shows the transmission types and modulation schemes corresponding to each supported data rate. Diverse combinations of both are applied to achieve various trade-offs of data rate and robustness. It has been shown, that configuring the data rate below 54 Mb/s limits the occurrence of packet errors [12].

TABLE I. 802.11g DATA RATES

Data Rate (Mbps)	Transmission Type	Modulation scheme
54	OFDM	64QAM
48	OFDM	64QAM
36	OFDM	16QAM
24	OFDM	16QAM
18	OFDM	QPSK1
12	OFDM	QPSK
11	DSSS	CCK2
9	OFDM	BPSK3
6	OFDM	BPSK
5.5	DSSS	CCK
2	DSSS	QPSK
1	DSSS	BPSK

QAM: Quadrature Amplitude Modulation
QPSK: Quadrature Phase Shift Keying
CCK: Complementary Code Keying
BPSK: Bi-phase Shift Keying

IEEE 802.11n can operate in the 2.4 and 5GHz band. It uses OFDM modulation scheme and achieves a maximum capacity of up to 600 Mbps, due to the MIMO

(Multiple-In-Multiple-Out) technology that takes advantage of multipath signal propagation, utilizing time and space diversity principles. The MIMO model is depicted in Figure 1.

IEEE 802.11e is a QoS extension in the MAC layer that has direct relevance to the industrial requirements on delay and performance constraints. It was demonstrated that IEEE 802.11e can lead to 50% reduced packet loss rate compared to 802.11n in the same test-bed [14].

The 2.4GHz band in Europe operates on 13 channels, where just 3 are non-overlapping (see Figure 4), whereas in the 5 GHz band all available 19 channels (for Europe) are non-overlapping.

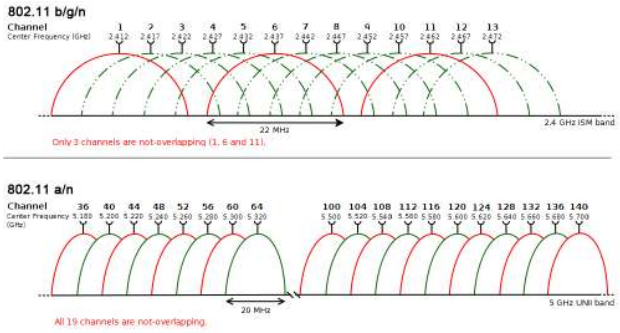

Figure 4. 802.11 channels

The 2.4 GHz ISM-band is also often used by other wireless applications that can be constant sources of interference, such as microwave ovens, radar systems, electrical welding machines and other wireless communication systems like mobile phones. It has been shown that such interference causes loss of data packets or a slowing down of transfer speed [12].

When using the 5 GHz Band, there is potentially much less interference. On the contrary, due to the higher frequency, it has a much narrower coverage, because obstacles limit range as frequency increases. The countermeasure to this is to increase transmission power for the 5GHz frequency band.

Another important parameter is the number of maximum retransmissions at the 802.11 MAC layer, which is set to 10 by default. Changing this number might be beneficial for certain applications.

5. SafetyNET p

SafetyNET p [6][15] according to IEC 61784-3-18 is an Ethernet-based fieldbus designed for safety related applications. The communication principle of SafetyNET p (IEC 61158 Type 22) is certified to SIL 3 according to IEC 61508 and can therefore be used in applications that safeguard operating and maintenance personnel.

The SafetyNET p real-time frame network (RTFN) version is based on the same mechanisms as standard Ethernet (MAC and IP Frames). It can achieve a system cycle time of around 1 ms for standard data and 4ms for safe data, which is mainly limited by the Ethernet access mechanism. Each RTFN participant knows its communication partner(s) and communicates with them in publisher/subscriber mode.

Safety integrity is ensured by the SafetyNET p communication endpoints. The transmission network is regarded as *black channel.* A well-known concept that indicates that the fail-safe communication is independent of the bus system and the network components in use. In [15], the concept of monitoring the safety integrity of a *black channel* through SafetyNET p is very well described. The communication parameters that are monitored for errors by SafetyNET p are listed in table II. If one of these parameters is violated, the SafetyNET p protocol will transit into fail-state. SHB response failures lead to fail-safe transitions, when they happen at least twice within a timeframe of 30 seconds.

TABLE II. DETECTION OF SAFETY COMMUNICATION ERRORS

Communication errors	Safety measures								
	Safety process data object (SPDO)			Safety heartbeat (SHB)					
	Timeout	CRC	Sequence	Timeout	CRC	Sequence	Response sequence	Response unfrequent	Delay Exceed
Corruption		X			X				
Unintended repetition			X			X	X		
Incorrect sequence			X			X	X		
Loss	X		X	X		X	X	X	
Insertion			X			X	X		
Masquerade			X			X	X		
Addressing			X			X	X		
Unacceptable delay (SPDO)	X								
Unacceptable delay (SHB)				X					
Unaccaptable delay (SHB-Response)								X	X

The SafetyNET p implementation in the “PSSuniversal PLC Controller” (by Pilz GmbH & Co. KG) can report the occurrence of the possible communication errors (see table II) via the syslog protocol (see Figure 10). This provides the opportunity to utilize these PLCs as measurement endpoints for the behavior of SafetyNET p on different communication channels. A special firmware was provided from Pilz, where the real transition into fail-safe state is disabled, but the event still written to syslog. This allows long term measurement without interaction when fail-safe-state was entered.

6. Experimental Setup: Safety over WLAN

Is an 802.11 wireless communication channel suitable for reliably operating a SafetyNET p (RTFN) application? This basic question brought the subject of this paper on the agenda.

6.1. SafetyNET p over a single wireless channel

First, this scenario was tried out with an initial test setup, where two "PSSuniversal PLC Controller" (by Pilz GmbH & Co. KG) were communicating to each other via a single 2.4GHz (802.11g) or 5GHz (802.11a) WLAN line-of-sight-connection between two Hirschmann BAT-54 Industrial WLAN access points (see Figure 5). The chosen SafetyNET p basic cycle time was 60ms.

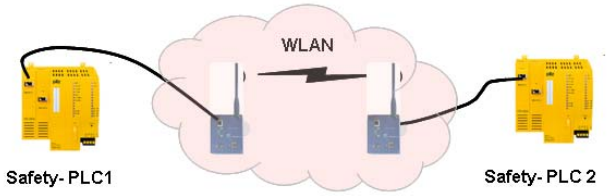

Figure 5. SafetyNET p over a single WLAN

Measurement criterion was the time duration until the system transits into fail-safe state because of insufficient safety communication. In the heavily interfered environment of Hirschmann's development department, the system never survived longer than 2 hours.

In a real application, transition to fail-safe-state would mean the interruption of the productive process, which would not be tolerable for the reason of an unreliable communication channel.

This proved by experiment that an ordinary 802.11 WLAN connection is not reliable enough for SafetyNET p (RTFN) communication, obviously because of sporadically occurring packet losses in the WLAN due to external radio interference, which gives support to the findings in [13].

6.2. SafetyNET p over a wireless PRP network

After the failures with single wireless channels, a different approach was investigated (see Figure 6). Two parallel redundant networks consisting of WLAN A (802.11a) and WLAN B (802.11g) are interconnected via PRP *Red Boxes* from zhaw [11] towards the end application devices. This forms a *black channel*, where the redundancy is not visible behind the red boxes towards the end devices PLC1 and PLC2.

This multi-radio diversity architecture applies some of the basic diversity techniques -on top of those already inherently used within a standard IEEE 802.11 channel- to further improve the overall quality of the combined wireless *black channel*:

- Space diversity through the use of two independent wireless channels with their antennas.
- Frequency diversity through the use of separated radio frequency channels in the 2.4 GHz and 5 GHz band in the two parallel wireless channels.
- Graceful performance degradation (GPD) through the duplicated wireless channel, which is a technique that still maintains functionality when a redundant structure fails, but at a lower performance.

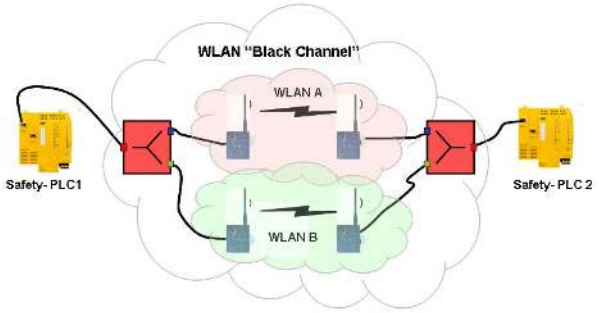

Figure 6. Parallel Wireless Redundancy

This approach worked very well immediately. In the same interfered environment as before, it run stable without any transitions into fail-safe-state over an observation period of a month. This clearly indicated that the stochastic fading of the two diverse wireless channels is not time correlated and the PRP mechanism compensates the fading consequences that appear in the single wireless channels.

7. Measurement Setup

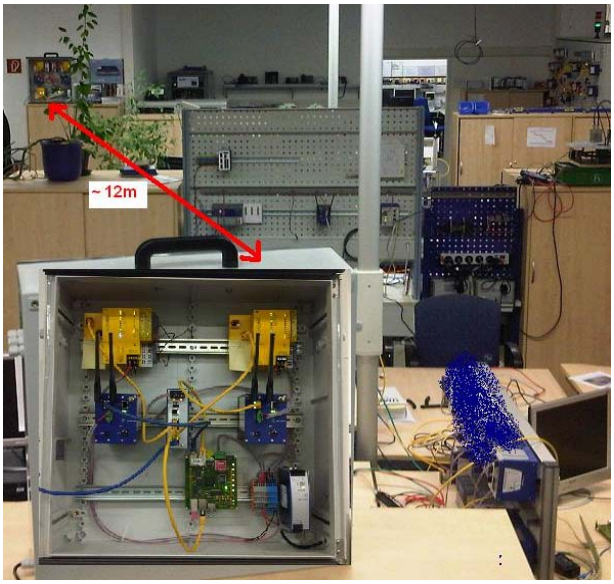

Figure 7. Measurement Environment

We built a measurement system (see Figure 7) that makes use of the Safety-PLC internal channel supervision mechanisms. The setup consists of four simultaneously

observed SafetyNET p connections as shown in Figure 8 and table I. The SafetyNET p connections PLC A – PLC B and PLC A – PLC D measure the single WLAN Channels A and B. SafetyNET p connection PLC A – PLC C is the data connection utilizing the parallel redundant system. Finally the SafetyNET p connection PLC A – PLC E is utilized as comparison towards the standard 802.3 behaviour. If in one of the SafetyNET p communications a violation of the protocol takes place (see table II), this is reported via syslog protocol towards the central syslog server (Figure 9). This method allows an easy correlation of the events on the individual channels.

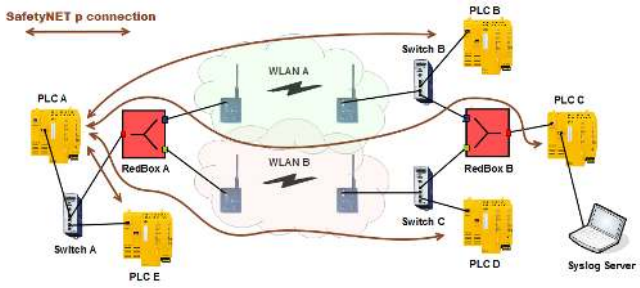

Figure 8. PLC Measurement Setup

TABLE III. MEASUREMENT SETUP

SafetyNET p connection	SafetyNET p nodes
WLANA	PLC A – PLC B
WLAN B	PLC A – PLC D
PRP	PLC A – PLC C
802.3	PLC A – PLC E

7.1. Reliability Measurement

Reliability is a measure of the continuous delivery of service according to specified conditions, or equivalently of the time to failure. It is expressed as MTTF and measured in time units.

$$MTTF = \int_0^\infty R(t)dt = \frac{1}{\lambda} \qquad (3)$$

The failure rate equals to 1/MTTF [16].

TABLE IV. MEASURED CHANNEL FAILURE RATES

No	WLAN	Channel No.	Cycle time	# Fail-safe transitions[a]		Failure Rate λ [1/h]	
I	A	40	60ms	4	3	0.024	0.018
	B	7		414		2.464	
II	A	36	30ms	40	0	0.238	0
	B	108		44		0.262	
III	A	36	15ms	12899	7	79.78	0.041
	B	108		16774		99.85	

a. measured over an observation period of one week

In measurement I with 60 ms cycle time we used 802.11a (Channel 40) for *WLAN A* and 802.11g (Channel 7) for *WLAN B*. Due to the highly occupied ISM frequency band in our environment (see Figure 10), fail-safe transitions in *WLAN B* were significantly higher compared to *WLAN A*, but still stochastically independent. An important result of this measurement was the occurrence of 3 fail-safe transitions in the overall channel due to the excessive delay of a few packets on *WLAN B*. The delay of some retransmitted packets was too high for the PRP protocol, which interpreted the packets as new frames instead as duplicates and forwarded them again, overtaking already delivered newer packets towards the application. The overall channel's *PLC C* responded with sequence failures and corresponding fail-safe transitions. These 3 fail-state transitions happened within 15 minutes in the one week observation period, thus indicating that some external distortion had taken place during this time. This revealed an inherent potential weakness of networks with alternative paths – the danger that packets may get out of sequence. Possible solutions to this problem would be an adjustment of the PRP implementation or a reduction of the WLAN retransmission settings.

For the following measurements II and III, both *WLAN A* and *WLAN B* were placed on the distant channels 36 and 108 in the 5 GHz frequency band, because of the occupation of the 2,4 GHz band.

In measurement II with 30 ms cycle time, the overall channel was faultless and both single channels had about the same amount of fail-safe transitions, but stochastically independent and thus not affecting the overall channel.

In measurement III with 15 ms cycle time, the failure rates in the single WLAN channels strongly increased. The overall communication could not stay free of fail-safe transitions and the limit of the presented approach seems to be reached, although the overall reliability is very good compared to the single channels.

7.2. Performance Measurement

In table V we see the results of a comparative measurement of the safety heartbeats roundtrip latency of the four safety connections in table III. For these measurements, we utilized a Hilscher netAnalyzer card for capturing the packets with precise timestamps as shown in Figure 11.

Both WLANs are in the 5GHz band, the measurement was taken over a period of ~20 hours with a cycle time of 30ms. Latency is calculated as time difference between SHB and SHB response at Switch A.

TABLE V. LATENCY MEASUREMENT

SafetyNET p connection	SHB roundtrip time[a]		
	Min [ms]	Max [ms]	Average [ms]
WLAN A	1.50	247.28	3.49
WLAN B	1.51	247.62	3.47
PRP	1.61	20.32	2.83
802.3	0.5	19.13	1.79

a. cycle time 30ms, observation period 20 hours

The average latency of the parallel redundancy path is more than 20% better than that of the single WLAN channels A and B. The maximum latency of the PRP path is significantly higher (~1 ms) than the 802.3 path, introduced to the inherent delays of the WLAN system. The most remarkable result here is the substantial improvement of the maximum latency by one order of magnitude compared to a single WLAN channel.

The single WLAN channels showed maximum latencies that lead to SHB response timeouts, but due to the stochastic independence, this never affected the overall channel.

In table VI and Figure 12 we see the results of a comparative jitter measurement of the four safety connections. The jitter analysis was made on the same data population as the latency measurement. But for jitter computation, the arrival time of the acknowledgement packet of the Safety Heartbeat was analyzed with IENetP [18].

As expected, the standard deviation of the jitter for a single WLAN channel is relatively high. The PRP path in contrast has nearly the same deviation behavior as the wired 802.3 Ethernet connection. Deviations at 100% (480 ms in Figure 12) indicate SHB response failures on the single WLAN channels.

TABLE VI. JITTER MEASUREMENT

Jitter of Safety Heartbeat Response			
SafetyNET p connection	**Deviation**[a]		
	Min [%]	Max [%]	Standard [%]
WLAN A	-7.04	101.42	2.00
WLAN B	-31.72	100.35	1.18
PRP	-6.52	6.82	0.17
802.3	-6.46	6.42	0.14

a. cycle time 30ms, observation period 20 hours

8. Conclusion and Outlook

We demonstrated by experiment that a diverse redundant Multi-Radio wireless architecture with PRP as combining method provides a solution for a significantly improved point-to-point-wireless communication channel, suitable for the reliable operation of SafetyNET p (RTFN) under certain conditions. The two redundant wireless channels behave stochastically strongly independent and always the better performing packet transmission reflects the overall performance.

We showed that the approach works well down to a cycle time of 30ms on standard WLAN settings. There is possibly much potential for further performance improvements by applying additional QoS measures on the WLAN settings. It became also clear that applications running over a PRP network and relying on the correct sequence of packets should be tolerant to a duplicated reception of already received packets. This can happen when the PRP window size is exceeded due to bad channel quality in one of the parallel WLAN channels.

The presented approach offers a lot of variability and further work is planned towards more measurements over longer time periods in different WLAN configurations and also with other real-time applications.

References

[1] IEEE 802.11-2011, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*; available at http://standards.ieee.org*

[2] A. Willig; "Redundancy Concepts to Increase Transmission Reliability in Wireless Industrial LANs (Extended Version)", *Technical Report TKN-05-002, TU Berlin, March 2005, available at http://www.tkn.tu-berlin.de*

[3] A. Willig; “Polling-based MAC protocols for improving real-time performance in a wireless network”; *IEEE Trans. on Ind. Electr., 50(4):806–817, August 2003.*

[4] D.G. Brennan, "Linear diversity combining techniques," *Proc. IRE, vol.47, no.1, pp.1075–1102, June 1959.*

[5] H. Kirrmann, M. Hansson, P. Muri; “IEC 62439 PRP: Bumpless recovery for highly available, hard real-time industrial networks“; *ETFA 2007.*

[6] Safety Network International; “SafetyNET p”; *available at http://www.safety-network.org*

[7] M.A. Kadhim, W. Ismail; “Performance Transmit and Receive Diversity Techniques for Different Modulation Signal”; *Journal of Telecommunications, Sept. 2010.*

[8] A.K. Miu, H. Balakrishnan, C.E. Koksal; “Improving Loss Resilience with Multi-Radio Diversity in Wireless Networks"; *ACM Mobicom, Sep. 2005.*

[9] H. Beikirch, M. Voss, A. Fink; “Redundancy Approach to Increase the Availability and Reliability of Radio Communication in Industrial Automation”; *ETFA 2009*

[10] B. Sklar; “Digital Communications: Fundamentals and Applications”; *Prentice Hall, 2000.*

[11] Zurich University of Applied Sciences, Institute of Embedded Systems: “Redundancy Box”; *available at http://www.ines.zhaw.ch/en/engineering/ines/high-availability/prp/solutions/redundancy-box.html*

[12] L. Seno, S. Vitturi, F. Tramarin; “Experimental Evaluation of the Service Time for Industrial Hybrid (Wired/Wireless) Networks under Non-Ideal Environmental Conditions”; *ETFA 2011.*

[13] T.Y. Arif, R.F. Sari; “Performance Comparison of Video Traffic Over WLAN IEEE 802.11e and IEEE 802.11n”; *UBICOMM 2010.*

[14] Salyers, Striegel, Poellabauer; “Wireless reliability: Rethinking 802.11 packet loss“; *WoWMoM 2008.*

[15] G. Cena, M. Cereia, A. Valenzano; ”Security Aspects of Safety Networks”; *ETFA 2011.*

[16] H. Kirrmann; “Fault Tolerant Computing in Industrial Automation”; *available at http://lamspeople.epfl.ch/kirrmann/Pubs/FT_Tutorial_HK_050418.pdf*

[17] NIST; “IENetP Test Tool”; *available at https://sourceforge.net/projects/ienetp/*

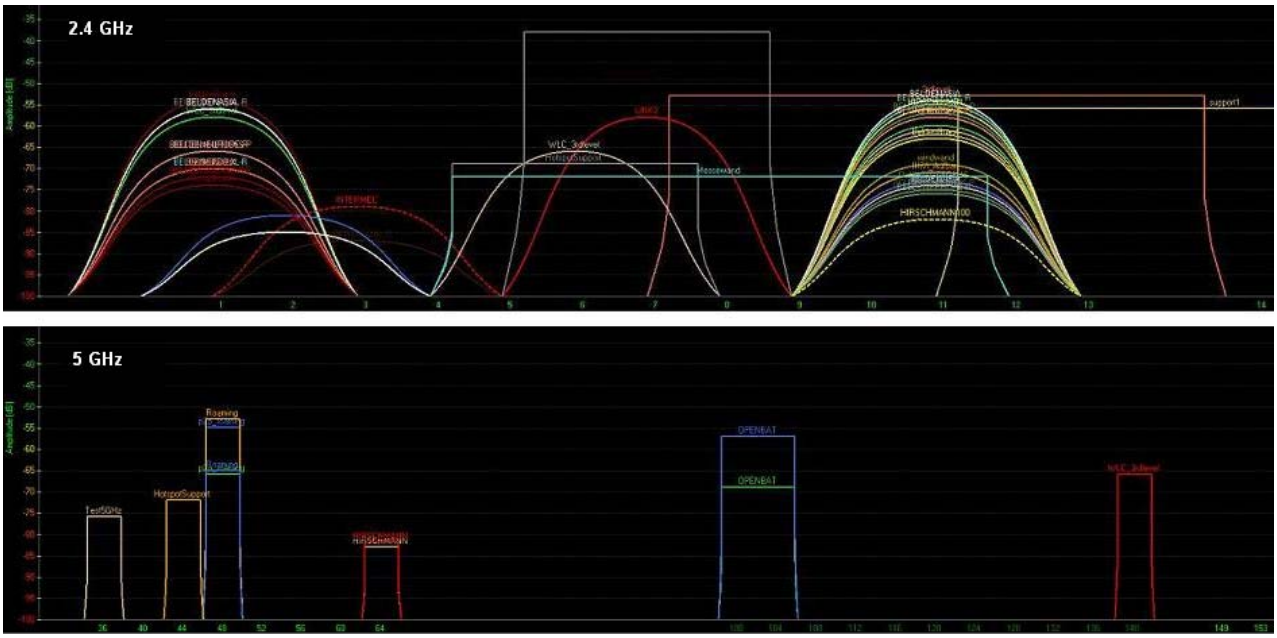

Figure 9. WLAN occupation in test environment

Syslog-Server		Safety-PLC			Syslog Message
date	time	IP	date	time	device name
2012-01-03	10:00:05	192.168.1.177,	<131>Jan 03	08:58:12	myEvalBoard3 PRP_TEST (A) ERROR_TYPE=SHB_Resp_Unfrequent, PID=160, IP=0.0.0.0
2012-01-03	10:00:05	192.168.1.177,	<131>Jan 03	08:58:12	myEvalBoard3 DiagItem(AB) (A) EventID=6C77477C38C22D72: deactivated Stoerung The failsafe stack has detected a conne
2012-01-03	10:00:05	192.168.1.177,	<131>Jan 03	08:58:12	myEvalBoard3 DiagItem(AB) (A) EventID=8A45E764B753DC57: deactivated Stoerung A (single) data connection is interrupt
2012-01-03	10:00:24	192.168.1.178,	<131>Jan 03	08:58:31	myEvalBoard4 PRP_TEST (A) ERROR_TYPE=SHB_Resp_Unfrequent, PID=60, IP=0.0.0.0
2012-01-03	10:00:24	192.168.1.178,	<131>Jan 03	08:58:31	myEvalBoard4 DiagItem(AB) (A) EventID=6C77477C38C22D72: deactivated Stoerung The failsafe stack has detected a conne
2012-01-03	10:00:24	192.168.1.178,	<131>Jan 03	08:58:31	myEvalBoard4 DiagItem(AB) (A) EventID=8A45E764B753DC57: deactivated Stoerung A (single) data connection is interrupt
2012-01-03	10:00:32	192.168.1.178,	<131>Jan 03	08:58:39	myEvalBoard4 PRP_TEST (A) ERROR_TYPE=SHB_Resp_Unfrequent, PID=60, IP=0.0.0.0
2012-01-03	10:00:32	192.168.1.178,	<131>Jan 03	08:58:39	myEvalBoard4 DiagItem(AB) (A) EventID=6C77477C38C22D72: deactivated Stoerung The failsafe stack has detected a conne
2012-01-03	10:00:32	192.168.1.178,	<131>Jan 03	08:58:39	myEvalBoard4 DiagItem(AB) (A) EventID=8A45E764B753DC57: deactivated Stoerung A (single) data connection is interrupt
2012-01-03	10:00:33	192.168.1.179,	<131>Jan 03	08:58:40	myEvalBoard5 PRP_TEST (A) ERROR_TYPE=SPDO_Timeout, PID=20, IP=192.168.1.175
2012-01-03	10:00:33	192.168.1.179,	<131>Jan 03	08:58:40	myEvalBoard5 DiagItem(AB) (A) EventID=8A45E764B753DC57: activated Stoerung A (single) data connection is interrupted
2012-01-03	10:00:33	192.168.1.179,	<131>Jan 03	08:58:40	myEvalBoard5 PRP_TEST (A) ERROR_TYPE=SHB_Resp_Unfrequent, PID=100, IP=0.0.0.0
2012-01-03	10:00:33	192.168.1.179,	<131>Jan 03	08:58:40	myEvalBoard5 PRP_TEST (A) ERROR_TYPE=SHB_Timeout, PID=70, IP=192.168.1.175

Figure 10. Syslog Messages as collected by the Syslog Server

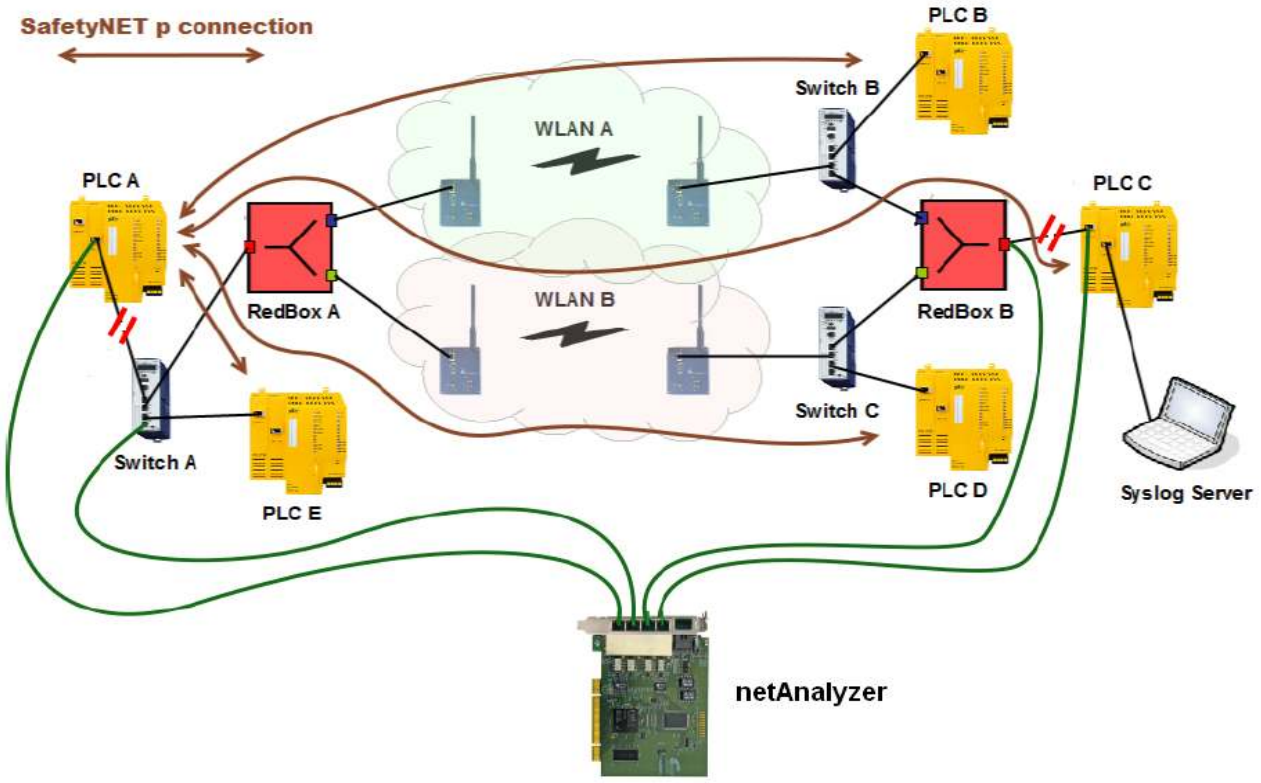

Figure 11. Modified test setup for latency and jitter measurement

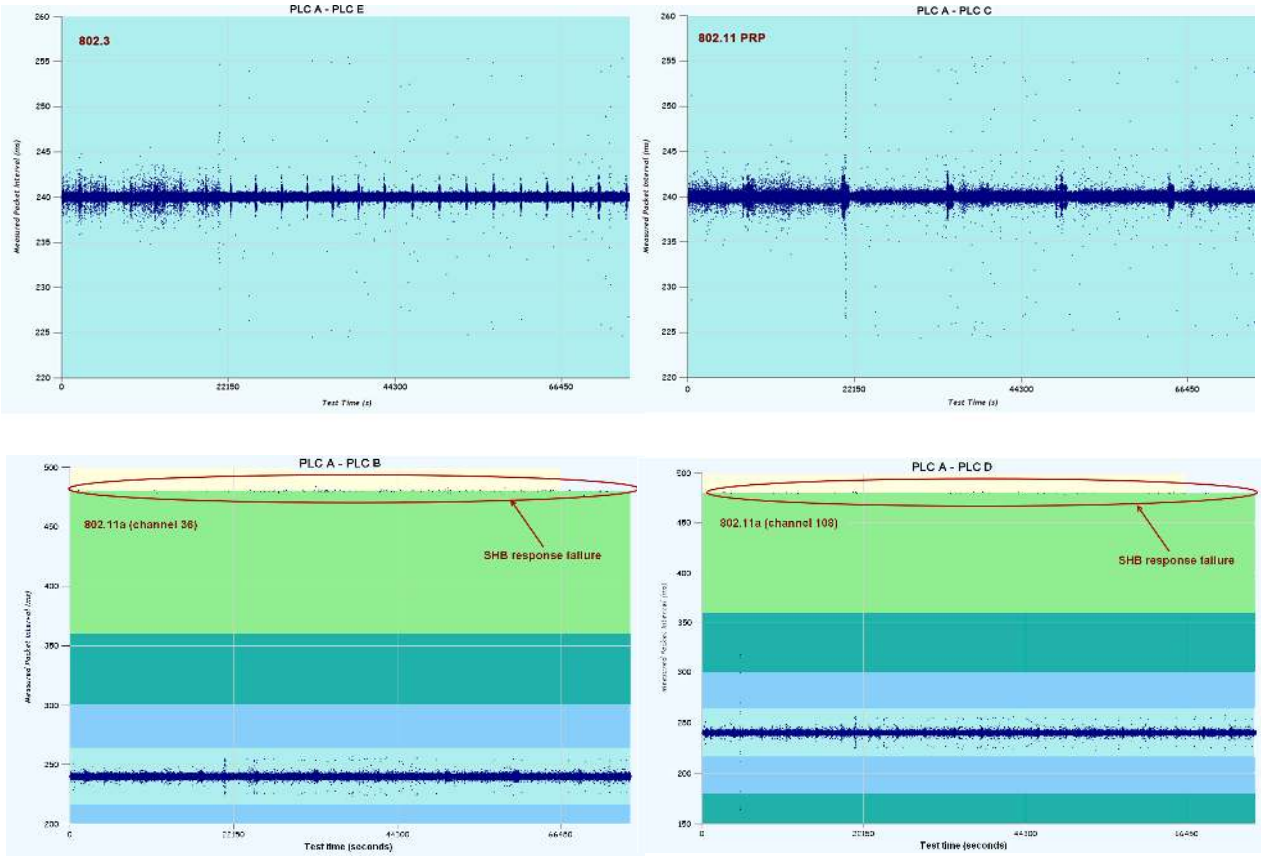

Figure 12. Jitter on the four measured channels (30ms cycle time, 20 hours observation period)