# Wireless Safety for Mobile Machinery

Ralf Kaptur (Hirschmann Automation and Control GmbH)

**Because of its flexibility and its ease of use, Wi-Fi based Ethernet communication has become state of the art also within automation networks. The fact that statistically 70 % of machine down time is caused by cable breakage or contact problems gives food for thought to mobile machine vendors as well. Furthermore wireless networks enable applications that are simply not possible with a cable connecting moving parts of a system. When connecting components of a safety related system – like PLCs or sensors and actuators – however, customers are facing serious issues. 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 lead to packet loss or exceeded and variable latency times due to retransmissions.**

In fact such consequences of stochastic channel fading can be compensated by the parallel operation of diverse wireless channels, applying frequency and space diversity techniques. A fault-tolerant wireless “black channel” can be achieved that is able to fulfill soft real-time requirements for safety applications by using standard WLAN components in combination with PRP (Parallel Redundancy Protocol) according to IEC62439-3. Appropriate reliability and performance characteristics have been derived from measurements on an experimental setup with SafetyNET p nodes and a field test using ICMP echo requests.

## Safety applications and black channel approach

Basic requirement for building up a safety system for risk reduction (according to IEC 61508 [7]) is the knowledge of the failure probabilities of all involved system components. A second design principle is failure diagnostics which means in fact error detection. Within mobile controls working in continuous mode, a detected error normally leads to a shutdown of the machine (safe state).

This approach basically also includes communication between the safety system components. A wired connection is normally supposed to be deterministic, which means:

- If there is no serious defect like a wire breakage detected, communication can start on request at any time within a certain interval.
- The data error rate is well known and doesn’t change during operation.
- All devices communicating on the medium are well known and do not change during operation as well.
- As regards wireless systems things are quite different:
- The wireless link is subject to changing environmental conditions like attenuation and reflection. Since this is always the case, a working link at time T is no prediction for an operational system at T+t.
- Also caused by $_{\text{external}}$ factors, the bit error rate can change during operation.
- Other devices using the same frequency band can influence the system or even manipulate communication (intentionally or unintentionally).

This is why a so called black-channel architecture, as indicated in fig. 1, is the only possible solution for wireless safety systems. A safety stack has to test the communication on a cyclical base to ensure availability. In case of any irregularities, the system switches into a fail-safe state which is often power off.

So to some extent a safety protocol stack transforms communication errors from being safety critical to being availability critical. This is why a safety stack reacts much more sensitive on communication errors and latency variations than any other application (except perhaps fast real time applications). Hence for proper operation it requires very stable communication timing.

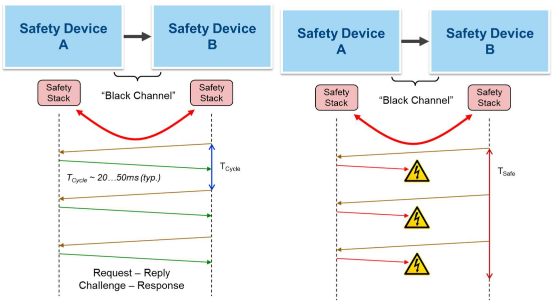


**Figure 1: Working principal of a safety communication stack**

Despite the mentioned availability issues, using a black channel architecture, especially in conjunction with Ethernet, provides of course also substantial benefits. Because of the transparent, nonsafety-relevant communication channel it's possible for example combining radio links and wired connections very easily by using standard off the shelf components (as shown in fig. 2)

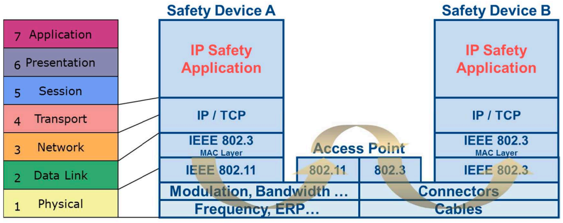


**Figure 2: Random mix of wired and wireless Ethernet technology**

## Redundancy for enhanced wireless network reliability

As mentioned before, safety applications are known as extremely time critical and error sensitive. Therefore they are ideal candidates to benefit from a boosted WLAN reliability.

The general idea of increasing the failure tolerance of an Ethernet network by using media redundancy and redundant paths is almost as old as the use of Ethernet for industrial communications, and so is the dilemma that – by definition – Ethernet technology's broadcast nature does not permit physical loops and therefore effectively forbids redundant communication paths. However, fault tolerance, which necessitates the use of redundant structures, is a vital basic requirement of many IT and automation systems. [1]

The spanning tree protocol (STP), the first algorithm designed to facilitate the use of redundant communications, was already published in 1990, albeit with switchover times of the order of many tens of seconds. Further protocols based on the underlying STP mechanisms were subsequently developed mainly with a focus on reducing the convergence time.

But even the last developments in this line of protocols like Fast MRP, which achieve switchover times of less than 20ms, have reached their natural limits. Eventually a new group of layer 2 redundancy protocols has overcome these limitations, providing seamless redundancy without any switchover time or packet loss.

## PRP approach compared to traditional bridge protocols

Talking about network redundancy, a basic distinction has to be made between layer 3 (routing) and layer 2 protocols (switching/bridging), both providing specific assets and drawbacks. If short switchover times are in focus, most probably a layer 2 redundancy protocol will be preferred.

In contrary to dynamic routing, layer 2 redundancy mechanisms create a temporarily static tree structure from the connections between the Ethernet switches and disable all those paths that are not a part of the active tree. This results in exactly one active path between any two devices. If the network is changed in any way, for instance by the failure of a physical connection, this is reported to all involved components by means of so called topology change notification BPDUs. The response to this is to recalculate the tree, activate the appropriate alternative paths and thus restore communications. During the reconfiguration period no data payload will be forwarded and all packets already on their way when the topology changes will be lost.

The needed reconfiguration time strongly depends on the network topology and the used bridging protocol. The typical switchover time for the classical spanning tree protocol (STP) of 30 seconds or even more was actually unacceptable for many IT networks and has been reduced by means of the rapid spanning tree (RSTP) to only a few seconds or even below one second.

Distinct improvements can be achieved by reducing the complexity of the network topology. This is why ring topologies have always been preferred for industrial network designs. By using Hiper Ring or the standardized media redundancy protocol (MRP) switchover times of less than 200ms can be achieved even for bigger networks. With appropriate hardware support and by utilizing FastMRP reconfiguration time can be reduced to less than 20ms eventually.

To be even faster than that, the redundant transmission has to be started basically before the network failure or reconfiguration has been detected. This means one has to send each packet twice from the start on different paths. Exactly this is the approach of the new PRP protocol, finally standardized by IEC 62439-3 in 2012 [2]:

As depicted in fig. 3, the parallel redundancy protocol (PRP) uses two independent static transfer networks. First, the egress traffic gets duplicated in a device called RedBox or dual attached node for PRP (DAN-P) and sent via two ports with identical source and destination addresses. On the other side a second RedBox has to ensure that only the first packet is forwarded and the second one is discarded.

Therefore each PRP packet contains a so called PRP trailer (6 bytes) with according sequence numbers between payload and frame check sequence. Fig. 4 shows the structure of the corresponding Ethernet protocol stack. It is a big advantage that PRP packets can be handled as ordinary Ethernet packets within the transfer networks, which are indicated as (W)LAN A and (W)LAN B in fig. 3. The devices within the redundant infrastructure don't have to support or even interpret PRP in any way.

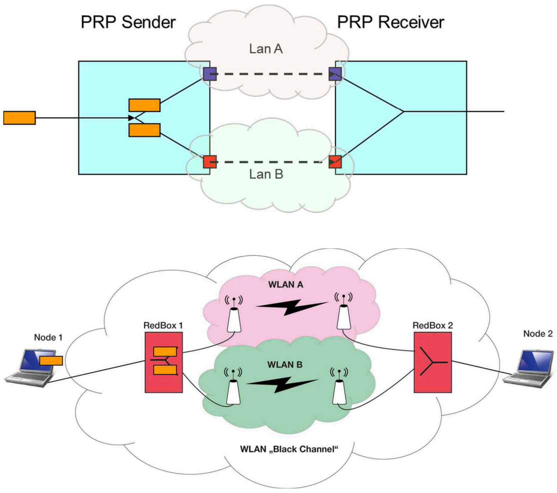


**Figure 3: PRP network redundancy [3]**

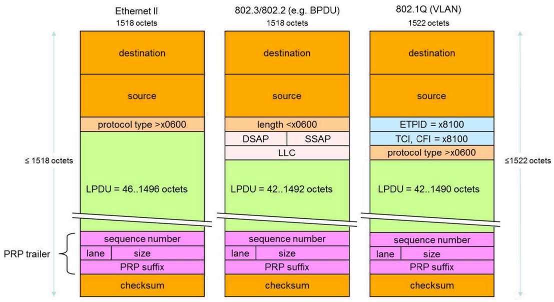


**Figure 4: Ethernet Protocol Stack with PRP Trailer [4]**

In fact PRP represents a standard solution for the final goal of interruption-free redundancy without any switchover time.

Even more than that, in case there isn't any network failure, latency is optimized by using the fastest path between source and destination.

## WLAN channel behavior and PRP diversity

IEEE 802.11 (Wi-Fi) based networks are basically the wireless extension of Ethernet based IEEE 802.3 local area networks. Higher layer LAN protocols and internetworking protocols, like TCP/IP, integrate seamlessly in this WLAN environment. Although state-of-the-art WLANs use very complex and efficient coding mechanisms, real-time requirements for industrial applications, such as guaranteed maximum latency for packet transmission, are often not reliably met in IEEE 802.11 channels.

Uncontrollable radio interference leads to packet losses and frame retransmissions on the nondeterministic wireless MAC layer, resulting in dropped packets or intolerably high latency on the application level, as depicted in fig. 5. For these reasons, WLAN according to standard IEEE 802.11 is widely regarded as an unsuitable communication channel for time critical safety applications such as SafetyNET p, openSAFETY, CIP Safety or Profinet Safety.

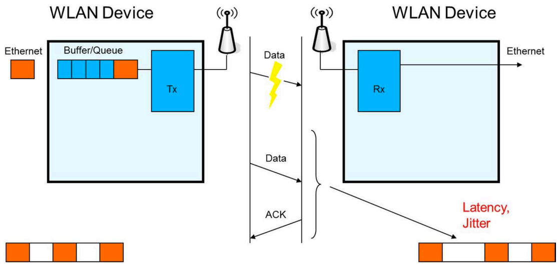


**Figure 5: WLAN channel behavior [3]**

Since the discovered packet losses and latency variations are normally uncorrelated, a combination of state-ofthe-art WLAN technology with PRP redundancy was developed as a new approach to improve the reliability of WLAN based transmission. The basic idea was to accompany the existing diversity and coding schemes on IEEE 802.11n level, which are focused on short term radio interference and maximum throughput, by a second redundancy mechanism on packet level with a focus on fault-tolerance or graceful degradation.

In order to create parallel redundancy channels, frequency diversity was considered. As shown in fig. 6, there are several options for using two WLAN radio channels: Two not overlapping single channels can be used or even two completely different frequency bands. Both approaches have been applied during the following tests.

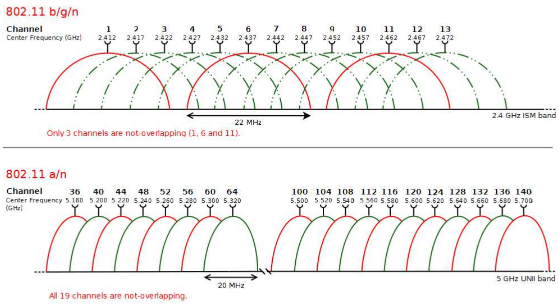


**Figure 6: Available WLAN channels [3]**

## Lab tests – wireless safety

As seen before, a safety protocol, designed for cable guided transmission, reacts very sensitive on latency variations (jitter) and packet losses and in case of doubt it shuts down the whole machine.
In order to prove the huge potential of PRP in combination with wireless LAN applications, a laboratory test setup with two safety controllers was used in the first step [3]. The network topology (see fig. 7) allowed for counting all fail-safe transitions of each individual radio channel and of the combined PRP link.

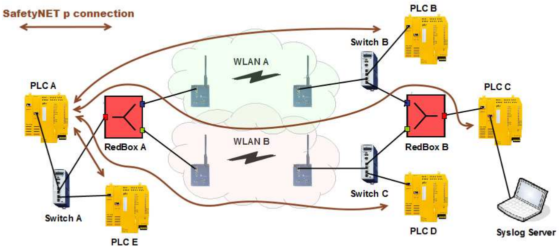


**Figure 7: Test setup for the reliability measurement [3]**

As the test results in tab. 1 are showing, the number of fail-safe transitions could be reduced massively by using PRP.
Depending on the configured controller cycle time, there were no fail-safe actions detected at all within a one week period or only very few of them, whereas for the single channels up to 100 per day occurred.

**Table 1: Safety fail-safe transitions per single WLAN channel and via PRP [3]**

| Test | WLAN | Channel No. | Cycle Time | #Fails-safe Transitions* | | Failure Rate λ [1/h] | |
|---|---|---|---|---|---|---|---|
| I | A (802.11a) | 36 | 30ms | 40 | 0 | 0.238 | 0 |
| | B (802.11a) | 108 | | 44 | | 0.262 | |
| II | A (802.11a) | 36 | 15ms | 12899 | 7 | 79.8 | 0.041 |
| | B (802.11a) | 108 | | 16774 | | 99.9 | |
| III | A (802.11n) | 36 | 15ms | 13079 | 2 | 77.9 | 0.011 |
| | B (802.11n) | 108 | | 22792 | | 135.7 | |
| IV | A (802.11n) | 36 | 20ms | 10659 | 1 | 63.4 | 0.006 |
| | B (802.11n) | 108 | | 9502 | | 56.6 | |

*observation periode = one week

The analysis of the heartbeat response shows a similar picture (tab. 2): Using only one WLAN channel leads to maximum deviations of more than 100% from the average, while less than 7% were measured on the PRP link. The shown roundtrip and jitter values for PRP are very close to those of a wired Ethernet link which was measured for comparison.

**Table 2: Safety heartbeat roundtrip times [3]**

| SafetyNET p Connection | SHB Roundtrip Time* | | | Jitter of Heartbeat Response | | |
|---|---|---|---|---|---|---|
| | | | | Deviation* | | |
| | Min [ms] | Max [ms] | Ø [ms] | Min [%] | Max [%] | σ [%] |
| WLAN A | 1.50 | 247.28 | 3.49 | -7.04 | 101.42 | 2.00 |
| WLAN B | 1.51 | 247.62 | 3.47 | -31.72 | 100.35 | 1.18 |
| PRP | 1.61 | 20.32 | 2.83 | -6.52 | 6.82 | 0.17 |
| 802.3 | 0.50 | 19.13 | 1.79 | -6.46 | 6.42 | 0.14 |

*cycle time 30ms, observation periode 20 hours

## Field tests – reliable WLAN

In order to confirm the lab test results also in harsh industrial environments, an appropriate test field was kindly made available by a leading German vendor of mobile machines. The radio link distance on the machine testing ground (see fig. 8) was approximately 80 m. The coverage area showed all characteristics that usually make WLAN service engineers feel cold sweat on their foreheads: A wireless enterprise network at 2.4 GHz, staff with mobile phones and probably Bluetooth head-sets, as well as Bluetooth based remote controls, using the legal maximum of radiated power. Moreover, mobile cranes were moved directly within the wireless range. As a consequence they inhibited free wave propagation and caused massive reflections and multipath distortions.

**Figure 8: Field test setup on a testing ground for mobile machines**

For this test, lasting one week in total, not only two channels within the 5 GHz band were used but two completely redundant frequency bands: 2.4 GHz and 5 GHz (IEEE 802.11.n). The thought behind this was that the connection would possibly not only be disturbed by a second standard compliant wireless service but a jamming transmitter. Furthermore, increased reflection diversity was supposed.

The test application used was a cyclic ICMP echo request. As indicated in fig. 9, the ping roundtrip delay was measured on the single radio links and the combined PRP link.

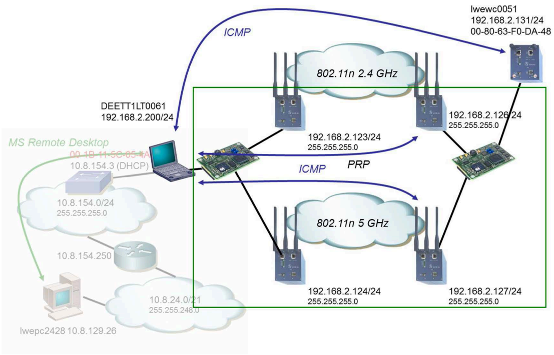


**Figure 9: ICMP test setup**

Fig. 10 represents the graphical summery of a typical testing day. The diagrams show the history of the echo latency data between the testing computer DEETT1LT0061 (IP 192.168.2.200/24) and the three ping targets within the two wireless networks and behind the PRP connection respectively. Each diagram shows both, the average latency [black curve] (calculated within a floating window according to the diagram resolution) and the related minimum and maximum values [light blue curves]. The latency area < 20ms is always marked green, the region between 20ms and 50ms is marked yellow and latencies > 50ms are marked light red. Lost packets are indicated by red vertical lines. Please note that the latency scaling differs from one diagram to another. Tab. 3 shows the summery of the three test sessions.

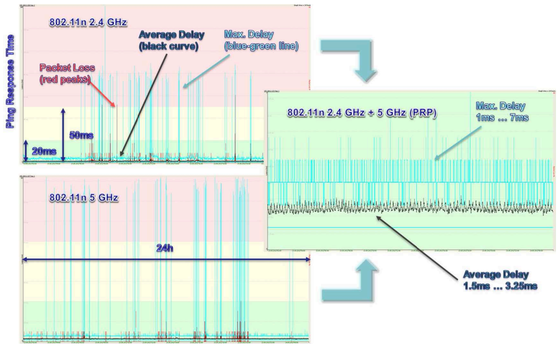
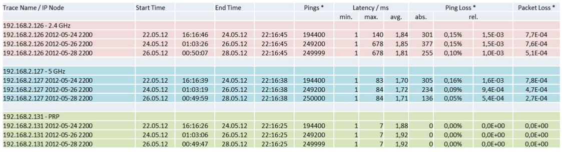


**Figure 10: Typical trend during the day**

**Table 3: Summery of the field tests**



| Trace Name / IP Node | Start Time | | End Time | | Pings * | Latency / ms | | | Ping Loss * | | | Packet Loss * |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | min. | max. | avg. | abs. | rel. | | |
| 192.168.2.126 - 2.4 GHz | | | | | | | | | | | | |
| 192.168.2.126 2012-05-24 2200 | 22.05.12 | 16:16:46 | 24.05.12 | 22:16:45 | 194400 | 1 | 140 | 1,84 | 301 | 0,15% | 1,5E-03 | 7,7E-04 |
| 192.168.2.126 2012-05-26 2200 | 24.05.12 | 01:03:26 | 26.05.12 | 22:16:45 | 249200 | 1 | 678 | 1,85 | 377 | 0,15% | 1,5E-03 | 7,6E-04 |
| 192.168.2.126 2012-05-28 2200 | 26.05.12 | 00:50:07 | 28.05.12 | 22:16:45 | 249999 | 1 | 678 | 1,81 | 255 | 0,10% | 1,0E-03 | 5,1E-04 |
| | | | | | | | | | | | | |
| 192.168.2.127 - 5 GHz | | | | | | | | | | | | |
| 192.168.2.127 2012-05-24 2200 | 22.05.12 | 16:16:39 | 24.05.12 | 22:16:38 | 194400 | 1 | 83 | 1,70 | 305 | 0,16% | 1,6E-03 | 7,8E-04 |
| 192.168.2.127 2012-05-26 2200 | 24.05.12 | 01:03:19 | 26.05.12 | 22:16:38 | 249200 | 1 | 84 | 1,72 | 234 | 0,09% | 9,4E-04 | 4,7E-04 |
| 192.168.2.127 2012-05-28 2200 | 26.05.12 | 00:49:59 | 28.05.12 | 22:16:38 | 250000 | 1 | 84 | 1,71 | 136 | 0,05% | 5,4E-04 | 2,7E-04 |
| | | | | | | | | | | | | |
| 192.168.2.131 - PRP | | | | | | | | | | | | |
| 192.168.2.131 2012-05-24 2200 | 22.05.12 | 16:16:26 | 24.05.12 | 22:16:25 | 194400 | 1 | 7 | 1,88 | 0 | 0,00% | 0,0E+00 | 0,0E+00 |
| 192.168.2.131 2012-05-26 2200 | 24.05.12 | 01:03:06 | 26.05.12 | 22:16:25 | 249200 | 1 | 7 | 1,92 | 0 | 0,00% | 0,0E+00 | 0,0E+00 |
| 192.168.2.131 2012-05-28 2200 | 26.05.12 | 00:49:47 | 28.05.12 | 22:16:25 | 249999 | 1 | 7 | 1,92 | 0 | 0,00% | 0,0E+00 | 0,0E+00 |

Although, as pointed out above, the environmental conditions were very challenging, both wireless connections worked astonishingly stable. During the night, packet loss rates were very low with roundtrip delays between 1ms and 8ms.

However, during the day the diagrams of the two single radio links show a lot of lost packets and increased roundtrip delays of more than 50ms. Thus, a safety controller, as used in the lab test, would probably have shut down the application permanently.

At the same time, the divers PRP connection doesn't show any packet losses. Even more important is the fact that the ping timing is very stable. With an average delay of 2ms for the ICMP mechanism, running in both directions over the combined link, the maximum latency is always less than 10ms.

Finally it can be stated that it's possible to connect time critical applications with high availability even over temporarily disturbed networks, in particular wireless LANs, by means of seamless redundancy switchover via PRP. This fact opens up new fields of application for industrial WLANs as for example the market of safety related controls.

## Mobile machine applications

The boosted wireless robustness paves the way for successful implementation of extremely stable and even safety related applications on various mobile machines.
On cranes for example, safe load indicators or other mission critical applications can leverage data connections between moving parts like the superstructure cab and the chassis or the main crane and the counter weight trolley.
Fig. 11 depicts a possible use case on a ship-to-shore gantry crane.

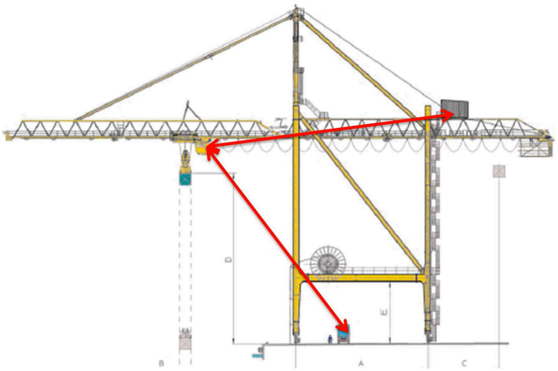


**Figure 11: Wireless communication on an STS container crane**

Finally not only fixed configurations on single cranes – replacing former wired connections – are possible. Rather than that, especially temporary ad-hoc connections between different machines best highlight the unrivalled potential of the wireless technology. Conditions which require more than one crane lifting a load simultaneously (see fig. 12) are an excellent example for this ability. A lot of accidents could be avoided by connecting all involved cranes to a centralized control system.

**Figure 12: Wireless communication supporting multi crane lift jobs**

## Summary

Ethernet redundancy with zero switchover time has become state of the art. The appropriate redundancy protocols like PRP, covered by international standards, are ready to use. Accordingly a lot of time critical higher level applications are leveraged by the massive gain of network availability. One special aspect is the design of extremely robust wireless LAN connections that are even suitable for reliable operation of safety-related controls. Test data taken in the lab and also outdoors under practical conditions within a machine park give proof of the boosted performance of newest WLAN technologies in combination with seamless redundancy mechanisms. It was shown that the safety approach works well down to a cycle time of 30ms with standard WLAN settings. There is possibly much potential for further performance improvements by applying additional QoS measures on the WLAN infrastructure.

Ralf Kaptur
Hirschmann Automation & Control GmbH
Stuttgarter Straße 45-51
72654 Neckartenzlingen
Phone: +49 7127 14-1693
Mobile: +40 173 2983276
ralf.kaptur@belden.com
http://www.hirschmann.com

Jürgen Bäsel
Hirschmann Automation & Control GmbH
Hertzstraße 32-34
76275 Ettlingen
Phone: +49 7243 709-3133
Mobile: +49 172 7331801
juergen.baesel@belden.com
http://www.hirschmann.com

## References

[1] White Paper – Media Redundancy Concepts, Hirschmann Automation and Control

[2] Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR), IEC 62439-3 ED. 2.0 B:2012, specification available at http://webstore.ansi.org

[3] M. Rentschler, P. Laukemann: Towards a Reliable Parallel Redundant WLAN Black Channel; WFCS 2012

[4] H. Kirrmann: Parallel Redundancy Protocol an IEC standard for a seamless redundancy method applicable to hard-real time Industrial Ethernet; IEC SC65C WG15 © 2011

[5] H.Kirrmann: HSR – High Availability Seamless Redundancy, Fault-tolerance in Ethernet networks, IEC 62439-3; IEC SC65C WG15 © 2012

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

[7] Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, IEC 61508 (2010-04) Ed. 2.0