RailCheck: Functional Safety for Wireless Condition Monitoring of Railway Turnouts and Level Crossings

Jan Sramota, Mary Ann Lundteigen, Stig Petersen, Amund Skavhaug
Department of Mechanical and Industrial Engineering
Norwegian University of Science and Technology
Trondheim, Norway
Email: {jan.sramota, mary.a.lundteigen, stig.petersen, amund.skavhaug}@ntnu.no

***Abstract*— Increasing demands for more cost-effective, reliable and safer railway infrastructure unavoidably bring up the need for transitioning from current preventive maintenance strategies to more efficient, predictive, condition-based maintenance models. Such a change requires large installations of sensors that continuously monitor key infrastructure and aggregate captured data for post-processing in the cloud. Due to the amount of assets to be supervised, novel approaches must be studied in order to find a viable solution that is deployable on this scale. Continuous surveillance is then a desired goal, as it is closely associated with big-data analytics and allows to predict upcoming issues and react to unexpected events. Infrastructure managers will gain much better overview as a result of large amount of highly representative data set-in-context; moreover, they will benefit from having supportive algorithms simplifying their determinations. This paper describes the safety-related measures performed on one such system; eventually intended to replace the routine inspections currently being carried out on railway points and level crossings.**

I. Introduction

Increasing demands for better transportation systems in the 21st century resulted in a trend called *smart transportation* and facilitated the emergence of *intelligent transportation systems*. These systems aim to minimise traffic problems, enrich stakeholders with prior knowledge, reduce travel time and cost as well as enhance passengers' comfort and their safety. Indeed, between today and 2050, major changes are expected due to previous increased activity in this area [1].

Speaking at the operational level, the European Rail Traffic Management System (ERTMS) [2], which provides a common framework for all railway traffic in Europe, was adopted and is now being implemented. The ERTMS comprises the European Train Control System (ETCS), railway adaptation of the Global System for Mobile Communications (GSM-R) [3][4] and the European Traffic Management Layer. Interestingly, work that started on ETCS in the early 90s revealed number of challenges that either affected or resulted in several safety-related and technological standards, including e.g. IEC 61508 [5], EN 50159, GSM-R and the forthcoming LTE-R [6]. It remains an open question whether or not LTE-R will be launched as a successor to GSM-R (as happened in South Korea), or if the next generation '5G-R' will be used instead. However, it is expected that ERTMS at level 3, having the potential to increase the capacity up to 40% on the current infrastructure [7], will revolutionise this sector.

At the infrastructure level, the transition from preventive maintenance to a more targeted approach so-called predictive condition-based maintenance would dramatically alter this segment. Predictive maintenance strategies use sensors that continuously monitor crucial parameters and in conjunction with analysed historical trends evaluate the life-cycle stage of the monitored parts. This allows precisely predict impending failures and use the railway infrastructure with a higher efficiency, resulting in lower costs and enhanced safety. This paper describes one such system called RailCheck, developed and built at the Norwegian University of Science and Technology (NTNU). This system monitors railway infrastructure by utilising remote sensors and big-data analytics to interpret approaching and imminent threats hard to detect otherwise.

II. Overall Risks & Hazards Overview

Train derailment and collisions are the most severe situations that may arise due to neglected maintenance and poor workmanship. They occur as a result of a number of distinct causes that can generally be classified as mechanical failure of track components (e.g. broken rails, cracked rails, broken gauge spreads), geometric failure of track components (e.g. rail climbing due to excessive wear, earthworks slip) and dynamic failure of train/track interaction (e.g. extreme hunting, vertical bounce, track shift under the train).

To prevent such events, railway tracks are regularly inspected by equipped measurement trains that use a combination of cameras and laser-based systems. These tools automatically evaluate the condition of the track and help identify mentioned faults before they can negatively affect performance or become a safety issue. Located problematic spots can then be manually inspected by the infrastructure managers (IMs) either from the camera footage or personally by the inspection in the field. This is a very convenient way how to effectively monitor and maintain this large and dense network. Unfortunately, most of these tools are limited just to the tracks, excluding points and level crossings (P&C), which have to be then still inspected solely manually. This in combination with a large number of these units, estimated to be one P&C per km of track (EU27) [8], makes the associated tolerable hazard rate (THR) difficult to maintain and demands for lower maintenance costs, believed to be an equivalent of about 0.3 km of the plain tracks [8], unable to achieve.

Stationary systems, as RailCheck, might be particularly helpful since they can be deployed on selected or remote objects that require more frequent or detailed surveillance. Long-term monitoring of key parameters of highly significant objects, such as endangered tracks, bridges, or P&C, would allow IMs to predict their response in time and react to sudden changes. These might be caused by insignificant random events as well as severe ones—e.g. floods, landslides or deliberate human actions. A reliable wireless sensor network (WSN) and classification algorithms are then the absolutely necessary to replace the regular inspections carried out today and fully transition from preventive to predictive condition-based maintenance. Due to the complexity of this system, only a monitoring part (WSN) will be further described.

III. System Definition & Operational Context

RailCheck, shown in Fig. 1, is a dedicated condition-based maintenance system built over a three-year period as part of the DESTinationRAIL H2020 EU-project. It consists of multiple wireless battery-powered sensors (WS) attached directly to the rail body and a gateway (GW) located on the catenary mast along the rails. The GW communicates with the WS in range at sub-1GHz frequency and creates a local cell that forwards data to the server (SE), often referred to as a cloud. The train/track interaction is automatically captured by the WS's accelerometers, when the train passes over the infrastructure with deployed sensors. Data are then transmitted through a low-power wide-area network (LPWAN) to the SE, where these data are processed and analysed. IMs can thus get a detailed near real-time overview over their assets.

The system outlined above has been primarily developed to clarify and provide an answer as to whether or not the current state of the art allows the design of an optimal WSN for transition from preventive to predictive maintenance on such a large scale. Any answer must not only take into account a number of distinct parameters, including economic viability, system reliability, overall system security and safety, but also meet all project-specified requirements. These demanded low-cost battery-powered wireless sensors that are capable of monitoring selected infrastructure, e.g. railway P&C, for a time-span of more than 5 years. Results of these efforts were published in 2018 [9], and revealed the necessity of addressing also the safety-related parameters of this system. This manuscript aims to identify the necessary steps to make this system safe and deployable in real traffic conditions without losing any qualitative parameters of the system.

RailCheck was primarily intended to be used for monitoring the rails' geometric quality and their wear. However, due to the selected detection method used, many track-related data, including the train's response, is captured. This allows to observe the overall picture of the track structure, and to a certain extent the state of the passing trains. Several of the train chassis faults, e.g. flat wheel or axle bearing failure, can be identified at an early stage, which in turn prevents further damage to the rails. Modified sensors may be also used to monitor land slides and other highly critical events which further enhances this system's detection possibilities.

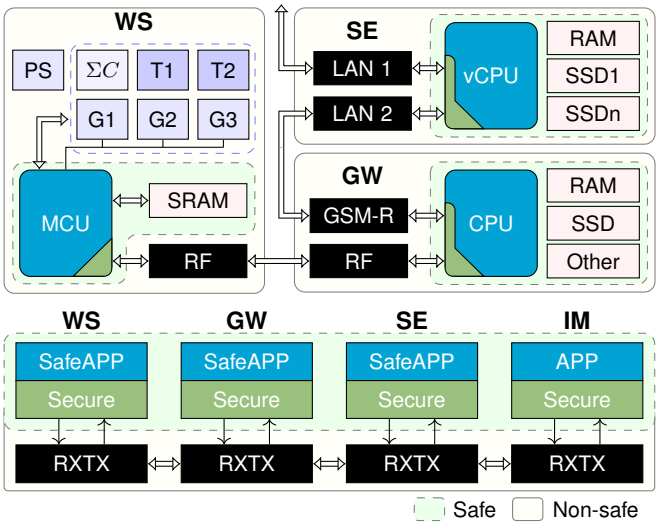

Fig. 1. RailCheck Schematic & Black Channel Concept

IV. Dysfunctional Analysis

The failure mode, effects and criticality analysis (FMECA) [10] were used to identify failure rates of different failure modes against the severity of their consequences while considering the barriers' effect. Please note that notation as A1 and F2 in Table I and in Fig. 2,3 represent the chapter in this section; B1 e.g. refer to the sub-chapter IV-B1.

A. WS Failures

The fundamental stress on low-cost and low-power consumption makes these sensors affordable and deployable on a mass scale. However, it is significantly more challenging to meet safety requirements and maintain expected reliability.

1) Casing: Housing failure, especially in the case of ingress protection (IP), may lead to several hazardous conditions. The battery might discharge in an undetected manner and a short-circuit may result in either a corrupted data or communication disruption. The same consequences may also include a moisture build-up inside the casing. These failures may be caused by random events such as poor workmanship, ageing of materials, exposure to excessive stress as well as by deliberate human actions such as vandalism.

2) Electronic: Hidden hardware/software (HW/SW) failures lead to severe catastrophic consequences that must be mitigated, optimally avoided completely. The sudden loss of power affecting large numbers of sensors, e.g. due to faulty updates, poses a real threat. The systematic failures are an even greater threat since they can hide the true condition of the monitored parts, and in certain cases remain undetected.

3) Security: Unauthorised physical manipulation is a severe threat since consequences of adversary actions can conceal true condition of the monitored parts. An adversary might try to gain knowledge by stealing one of the sensors from the remote areas. This would not go undetected, neither would it be prevented. Adversary would gain knowledge about the HW and could then try to reveal the SW installed on the WS. Adversary could learn about the defence measures in place and try to prevent triggering them the next time.

B. WS Barriers

Measures implemented to either prevent or mitigate the consequences of failures, identified in Section IV-A, are referred as barriers and are described in the following sub-chapters. The failure/barrier relationship, shown in Fig. 2,3, has been taken into account for the calculations in Section V.

1) Displacement Detection: The WS's vibration and movement are monitored by the 3-axis accelerometer that is most of the time set in a sleep measurement mode with a sampling frequency of 10 Hz. Any response over the selected threshold at any axis triggers the full measurement mode, allowing it to determine the source of this acceleration. Events are then classified based on their acceleration and wireless data. Identified safety-related events that differ from the train response, e.g. vandalism and unauthorised manipulation, are immediately reported to the system operator. All data provided after an identified unauthorised manipulation are treated as unreliable, and IM intervention is required.

2) Physical Barrier: The casing provides a passive barrier against deliberate and random failures A1 that may develop into liquid ingress A2, and a barrier against unauthorised manipulation A3. The casing is made of solid material PA2200 [11] containing acceptable material properties that include a high level of strength and firmness, strong chemical resistance, and excellent long-term stability. The Charpy impact strength, according to standard ISO 179/1eU [12], is a 53 kJ/m^2 which is expected to be sufficient to withstand most relevant impacts. Mechanical connections are protected by Acrylonitrile-Butadiene Rubber (NBR) o-ring sealings that might also be permanently sealed. The current casing is fitted with an unprotected dipole antenna that may be damaged and must be replaced with a build-in version covered by the casing. This casing will then be certified for IP mark IP64 according to the IEC 60529 [13].

3) Reprogramming Lock: WS's firmware is guarded by a code protection feature that locks in the device's reprogramming and reading its memory. In addition, the microcontroller's PCON register is monitored to identify sudden resets, reprogramming attempts or any other unexpected behaviour e.g. stack over-/underflow. The firmware is periodically verified to ensure the SW's integrity. The WS reacts to identified unauthorised manipulation by invalidating the cryptography keys on the GW and by erasing the WS memory. This prevents adversary from learning about defence mechanisms in place and becoming capable to gain access to the network.

4) HW/SW Integrity: To avoid data corruption originating from a sensor malfunction, hardware is equipped with multiple redundant sensors, as shown in Fig. 1. Temperature is measured by two sensors T1 and T2, acceleration by two or three accelerometers G1-3 measuring different magnitudes. First, this action increases the WS's usability, since WS can be deployed in various places and measures a wider range of accelerations. Secondly, it improves reliability, since the output values can be compared with one another to identify the corrupted data. This is performed directly by the microcontroller to prevent higher battery consumption caused by the additional wireless traffic. The microcontroller also

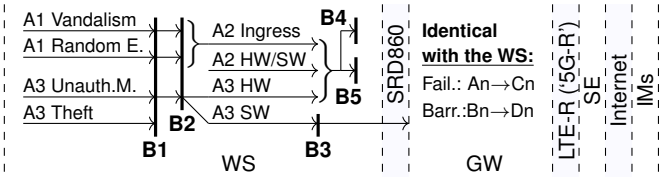

Fig. 2. HW/SW - Failures (An) & Barriers (Bn)

communicates with the peripherals strictly digitally, by the Serial Peripheral Interface (SPI), to prevent possible transmission errors or unauthorised manipulation. Communication error flags are monitored to detect any possible malfunctions. Self-diagnostics of the electronics are periodically performed to validate the calibration of the sensors and to detect defects.

5) Power Supply: Power diagnosis is an essential step to achieving reliable WS operation. The DC/DC converter with integrated coulomb counter, shown in Fig. 1 as ΣC, monitors the amount of power that has been used in order to estimate how much battery power is left. This allows the battery's entire life-cycle to be monitored with relative ease in order to prevent an unexpected power loss. The coulomb counter overflow, reach of the coulomb counter threshold and AC(ON) time overflow, which might indicate a low capacity of the built-in battery, are all supervised.

C. GW Failures

The GW is vulnerable to similar threats existing for a WS, as described in Section IV-A, but at the same time it can be better protected against deliberate and random threats. This is due to the possibility of attaching the casing to a less accessible location on a catenary mast along the rails, not as strict requirements for a low-cost and low-power consumption, and stricter requirements for overall security. If a GW gets compromised, all underlying infrastructure is affected, which jeopardises the whole local cell. This is caused by the fact that the higher we move towards the SE on the communication chain, the stronger the security must become in order to avoid larger and more severe consequences.

D. GW Barriers

The GW's failures/barriers model is in general identical to the one for WS shown in Fig. 2. What differs is the evaluation of frequency and severity for each failure that is seen in Table I and the way in which these barriers are implemented. These differences are summarised in following sub-chapters:

1) Displacement Detection: Detection is performed by the same means as for WS since this method provides accurate information about any atypical activity related to the casing.

2) Physical Barrier: The GW is enclosed in an industrial grade polycarbonate cabinet with an ingress protection rating IP66 (EN 60529) and impact resistance IK10 +35°C /IK08 -25°C (EN 62262). The door is protected by a key lock.

3) Reprogramming lock: The GW has a Linux distribution running on its HW that is responsible for both data consistency and overall data security. The data are stored in encrypted form, and access to the system is protected by the user password. GW uses Hypertext Transfer Protocol

Secure (HTTPS) requests to communicate with the SE and packet-based communication encrypted by an AES while communicating with the WS. All individual WS access keys to the network are securely stored in the GW's memory.

4) HW/SW Integrity: Barriers D3 and D4 from Fig. 2, identical to a B3 and B4 for a WS, are merged into a single barrier. This is described further above in Section IV-D3.

5) Power Supply: The GW is powered by a battery that is charged by a solar panel. To prevent sudden power loss, both the battery charging and power consumption are constantly monitored and optimised according to the current conditions.

E. Communication Failures

RailCheck uses the *black channel* concept, shown in Fig. 1, due to its favourable property that allows the use of unsecured public networks. This puts the RailCheck into Cat. 3 transmission system that must use strong countermeasures against the generic seven threats (G7T). These are known as (1) Repetition, (2) Deletion, (3) Insertion, (4) Re-sequencing, (5) Corruption, (6) Delay and (7) Masquerade. Moreover, EN 50159 describes 24 hazards, shown in Table A1 [14], that might lead to a communication failure. These 24 hazards are then classified into the G7T and must be prevented by well-known mechanisms *proven-in-use*. It is assumed that all threats except delay can be effectively prevented. The delay's severity is determined by its nature and how long it lasts:

1) Temporary Outages: These may be caused by randomly occurring environmental events, such as rain, lightning, solar radiation as well as by other electronic systems e.g. due to another active transmission on the same channel or another source of interference. These events are ranked as insignificant due to their temporary nature. It is not expected that these phenomena will result in outages longer than a couple of hours or days unless they simultaneously cause a partial or total traffic disruption. In these cases, the infrastructure would be physically monitored by other means.

2) Long-term Outages: These interruptions are labelled by severity category *critical* or *catastrophic*, due to their capacity to cause long-term outages. A typical attack comprises an entire spectrum jamming, which is a severe denial-of-service attack against wireless medium. It can be detected; however, it cannot be prevented. The source of interference must be actively tracked down and manually terminated.

F. Communication Barriers

Security events having direct consequences to a safety are handled in accordance with the 'Table 1 from EN 50159' [14]. The G7T from Section IV-E are then prevented by a combination of (1) cryptographic techniques, (2) safety code, (3) identification procedures, (4) feedback-messages, (5) source and destination identifiers, (6) timestamp, timeout and (7) sequence number. Since the *black channel* is used, packet creation and encryption must be performed already at the safe layer, which is in most cases implemented directly at the safe-microcontroller. The transmitter radio, shown in Fig. 1 as RXTX, then receives only cipher-text data. These cannot be manipulated and are simply forwarded to the communication channel. This so-called *end-to-end encryption* removes special requirements on hardware beyond the safety layer and simplifies the overall certification process.

Fig. 3. Communication Delay - Failures (En) & Barriers (Fn)

In addition to the above mentioned mandatory mechanisms required by the standard, other methods are deployed at the endpoints and have a positive effect on transmission efficiency, battery life, resistance to random events. Indirectly, they have also a positive effect on overall security and safety. These measures are outlined in the following chapters:

1) SRD860 (WS ⇔ GW): GW continuously monitors wireless communication on all channels and routes the communication with the WS over the most reliable set of links. Communication logs are aggregated at the SE for further analysis of any possible threats. Listen Before Talk (LBT), Adaptive Frequency Agility (AFA) and Adaptive Data Rate (ADR) controls are all used on both ends to achieve maximum permeability. In addition, WS is equipped with a simple algorithm monitoring the received signal strength indicator (RSSI). If the RSSI reaches the defined threshold, or WS loses its connection with the GW, WS sets the transmitting power to a maximum level of 10 dBm and lowers the transmitting data-rate down to a minimum value of 1 kbps. This is done in order to increase the the signal's transmission, thus increasing the link-budget. Afterwards, WS transmits the request to communicate over another set of frequencies. If a transmitted message stays unacknowledged on all channels, the device falls into a deep sleep mode to preserve the battery-life, having a scheduled wake-up call for another attempt. Communication attempts then decrease by factor 2 to a minimum period of one attempt every 12 hours.

2) LTE-R or upcoming '5G-R' (GW ⇔ SE): Regardless which of these protocols are finally used, both of them will be adapted and certified for railway safety-critical communication and implemented in accordance with the EN 50159 up to the SIL 4. Both will also be operated by a railway wireless service provider in a licensed spectrum, which further lowers the probability of interference with other systems. Since these networks are assumed to be safe and secure, and will be used just as a service, no other measures are taken.

3) Internet (SE ⇔ IMs): Communication with stakeholders is secured by the standard authentication and cryptographic protocols as they are used e.g. in communication with internet banking services. While this does not require a safe communication concept, communication must still remain secure. IMs establish the HTTPS connection with Transport Layer Security ($\geq$TLS 1.2) and are authorised by the two-step authentication process. IMs are then granted access based on their role in the system. Safe communication is not required since the IMs have no right to change the sensor data; indeed they are only allowed to display and evaluate these data. Due to internal procedures, their actions will not cause any dangerous situations to arise.

V. Safety Integrity Level (SIL) Requirements

This section specifies how system requirements arising from previous chapters are allocated and elaborates analysis of system to be protected—railway P&C, and analysis of the monitoring system—RailCheck. While the condition-based maintenance system RailCheck is comprised of two parts; the monitoring part (WSN) and the big-data analytics, only the WSN part has been sufficiently developed to this moment.

A. Analysis of the System to be Protected—P&C

The vast majority of railway points today are equipped with a point machine—a device to remotely operate a turnout. This type of point must be protected by a safety function (SF), which puts the unit into a so-called *equipment under control* (EUC). Unacceptable risk arising from the EUC is handled by the SF responsible for achieving and maintaining the safe state. As regards turnout, SF 'SKF 2' [15] ensure that the railway point remains locked and provides the correct information about its position and status of locking. This function is part of the train's control and therefore part of the signalling system. RAMS requirements define seven hazards against which the point equipment must protect—(1) the wrong position, (2) the correct position with too much tolerance, (3) the correct position with missing locking, (4) accidental unlocking, (5) track width reduction, (6) track gauge expansion and (7) incorrect information on locking and positioning of the locking equipment. These hazards have an acceptable occurrence rate associated with the worst case scenario, train derailment, assigned to THR=10^{-8}/h [15]. Assuming continuous operation, this is the equivalent of one failure per 1000 years and it is achieved by routine inspections, maintenance and by SFs. RailCheck's objective is to replace most of these inspections currently being performed on P&C by condition-based maintenance. RailCheck must therefore be at least as good as the traditional regular routine inspections carried out on P&C today.

To ensure the safety of this complex system, standards EN 50126, EN 50159 and IEC 61508 were examined and found to be relevant. Simultaneously, the EN 50128 and EN 50129 were assessed and excluded since they are more applicable for components that belong to signalling systems. RailCheck is an exclusive part of the maintenance system and will not play any direct role in the execution of the SFs.

B. Analysis of the Monitoring System—RailCheck (WSN)

The service life (SL) of rails is primarily determined by wear, plastic flow and defects. For example, wear mostly occurs on the gauge face in sections with high wheel-flanging forces e.g. when the train changes the track on a turnout. Certain wear is also caused by wheel/rail interaction on running surfaces due to maintenance activity, such as grinding. Plastic flow is a result of when wheel/rail contact stress exceeds the strength of the material. Rail defects happen due to many reasons and are a major concern. If they go undetected, they can grow and lead to unnecessarily expensive maintenance or, in a worst-case scenario, cause rail failure. Due to various improvements having been made to prolong rails' SL, the number of defects has in general increased [16]. All these factors negatively affect expected SL and in long-term undetected pose a threat to safety.

TABLE I
FMECA Analysis

HW	Failure	Cause	S	FR_I	RRF B1	RRF B2	RRF B3	RRF B4	RRF B5	FR_F
WS	A1 Casing	Vandalism	1	10^{-6}	0.1	0.6	-	-	-	10^{-7}
		Rand.Eve.		10^{-7}	0.6	0.1	-	-	-	10^{-8}
	A2 Electronic	IP Failure		10^{-7}	← incl.		-	0.1	0.1	10^{-9}
		HW/SW		10^{-8}	-	-	-	0.1	0.1	10^{-10}
	A3 Security	UM – HW	2	10^{-9}	0.1	0.6	-	0.1	0.1	10^{-12}
		UM – SW		10^{-9}	0.1	0.9	0.1	-	-	10^{-11}
		Theft	1	10^{-7}	0.1	-	-	-	-	10^{-8}
Wireless Medium SRD868		Long-term	3	10^{-10}	-	-	-	-	-	10^{-10}
					-	-	-	-	-	
GW	C1 Casing	Vandalism	1	10^{-8}	0.1	0.1	-	-	-	10^{-10}
		Rand.Eve.		10^{-8}	0.1	0.1	-	-	-	10^{-10}
	C2 Electronic	IP Failure	2	10^{-10}	← incl.		-	0.1	0.6	10^{-11}
		HW/SW		10^{-8}	-	-	-	0.1	0.6	10^{-10}
	C3 Security	UM – HW	3	10^{-8}	0.1	0.9	-	0.1	0.9	10^{-11}
		UM – SW		10^{-8}	0.1	0.9	0.1	-	-	10^{-10}
		Theft	1	10^{-7}	0.1	-	-	-	-	10^{-8}
Wireless Medium GSM-R		Long-term	4	— Not Relevant —						
SE	Electronic Security	Unauth.M. HW Failure	4	— Not Relevant —						
WAN Internet		Long-term	3	— Not Relevant —						
IMs	Security	Unauth.M. HW Failure	1	— Not Relevant —						

HW (Hardware); **FR_I/FR_F** (FailureRate–Initial/Final) [h^{-1}]; **S** (Severity): 1-Insignificant, 2-Marginal, 3-Critical, 4-Catastrophic; **RRF** (RiskReductionFactor): 0.1-Most Likely Prevented, 0.3-Rather Prevented, 0.6-Rather Failed, 0.9-Most Likely Failed; **Assumptions** [n]: WS250k, GW5k, SE1; **UM** (Unauthorised Manip.) **Note**–Only relevant severe failures are stated.

In order to calculate the values in Table I, THR must be properly stated. However, rail material has no specific SIL requirement and statistics records only track the failure rate on regularly inspected and maintained tracks. Moreover, there is no clear guidance given in either EN 5012x standards or technical regulations concerning THR assignment for condition-based monitoring systems. Discussions with contact personnel from the railway sector indicate that there are no internal guidelines on this topic, either. A majority of the systems used today are deployed as merely an additional monitoring step in regular inspections; therefore, safety-related parameters are not addressed. We have either not found any papers that take up whether or not condition-based maintenance should be assigned SIL requirements when it replaces routine inspections, or when inspections are extended to intervals so that defects may be expected during the period where only condition monitoring is available. As a result, current approaches to SIL allocation do not yet seem to be fully suited to these systems.

A review of other available technologies for condition-based monitoring suggest either no SIL requirement or SIL 1 to SIL 2. The systems using a SIL requirement are related to the monitoring of bearings for train wheels [17]. Our conclusion is that SIL requirement will be required at some point by IMs. Based on our review of current technologies,

a SIL 1 requirement for low-demand system as shown on Eq. 1 appears to be reasonable, as a design basis for a WS deployed on a single P&C, SIL 2 might then be achieved with redundancy by deploying several WSs on a single P&C.

$$THR = \left(\sum_{i=1}^{n} FR_{Fi} \right) < 10^{-4}/h \qquad \textit{(SIL 1)} \quad (1)$$

To estimate the failure rate by frequency of its occurrence for all failures from Table I, the following is assumed. Each national railway IM conducts its own RailCheck system, which defines the maximum number of WSs in the system. The European largest railway network, in Germany, comprises 44k km of railway tracks with an estimated one P&C per km of rails [8]. This equals an estimate of ~44k P&C, which are then each equipped with four WSs in case of railway turnout and by one or two WSs in case of level crossing. The system could therefore consist of ~250k units of WSs. The SL of WS is defined as a continuous operation 24 hours a day for an entire year over a time span of 10 years, which equals 87.6k hours. Next, to estimate the number of gateways in the system, we assume that there is on average one gateway per 50 WSs, which produces ~5k GWs. So e.g., the initial failure rate (FR_I) for failure A2 Ingress is calculated assuming that $<$2.5% of all WSs fails during SL due to IP failure:

$$FR_I = \frac{Failures}{SL \times Units} = \frac{6k}{87.6k \times 250k} = 2.74 \times 10^{-7} \quad (2)$$

For estimations of the final failure rate (FR_F) after the effect of barriers, FR_I is multiplied by the risk reduction factor (RRF), which reflects the effect of each independent barrier.

$$FR_F = FR_I \times RRF = 274n \times 0.1 \times 0.1 = 2.74 \times 10^{-9} \quad (3)$$

An analysis of the entire communication chain has been excluded, since well known mechanisms *proven-in-use* are already in place. This analysis has primarily focused on custom-made and physically exposed units—WSs and GWs.

VI. Conclusion

The transition from wired to wireless communication is an overall trend in all areas of human activity. In the railway domain, this was define already in the early 90s by setting up the working group on GSM-R as a result of work on ETCS. While the main motivation was to resolve interoperability across the national safety systems incompatible over the borders, it is inevitable that next-generation railway networks will moreover to the current state also incorporate a public data transmissions. Communication with the rolling stock, safety-critical infrastructure and other non-safety related systems will then all coexist under one common roof. This will allow safe connections with trains and turnouts, transmit camera surveillance streams from trains and stations and provide passengers WiFi while travelling. This will positively affect a whole range of current and impending applications and it will allow new sustainable deployments, including the emergence of smart-points—a turnout capable of utilising next-generation communication networks such as LTE-R or '5G-R', and accommodate additional applications. This will minimise the overall costs of systems like RailCheck so they will no longer represent any significant costs even for mass-scale deployments. Until then, RailCheck can be used for (1) remote monitoring of selected turnouts requiring additional surveillance and (2) as a multi-purpose platform for developing robust algorithms for condition-based maintenance.

This paper has demonstrated a certain number of the initial steps required for applying IEC 61508, EN 50126 and EN 50159. Emphasis was placed on clarifying the context of use, potential hazards and SIL requirements that might apply to this system. In addition, an initial dysfunctional analysis has been made to justify the idea that it seems possible to meet the suggested SIL requirements with respect to systematic and random HW failures. However, further work should include a more detailed analysis of both failure rate estimates as well as other measures that are imposed by the SIL requirements. For instance on the avoidance and control of SW faults in the development of the application program. This paper has also reviewed ways to consider security along with safety design. The exposure of such a system due to wireless technology and devices that may be accessed by anyone entering the tracks means that no such system will be safe if it is also not secure.

References

[1] European Commission. *Delivering an effective and interoperable European Rail Traffic Management System (ERTMS)-the way ahead*. SWD(2017) 375 final. EU, 2017.

[2] European Commission. *ERTMS–Delivering Flexible and Reliable Rail Traffic*. EU, 2006. ISBN:92-79-00584-7.

[3] EIRENE-GSM-R Functional Group. *Functional Requirements Specification Version 8.0.0*. UIC, 2012. ISBN:2-7461-1831-7.

[4] EIRENE-GSM-R Operators Group. *System Requirements Specification Version 16.0.0*. UIC, 2012. ISBN:2-7461-1832-4.

[5] IEC. IEC 61508:2010–Functional safety of E/E/PE safety-related systems. *International Standards and Conformity Assessment for all electrical, electronic and related technologies*, 2010.

[6] K. Guan, Z. Zhong, and B. Ai. Assessment of LTE-R Using High Speed Railway Channel Model. In *Third International Conference on Communications and Mobile Computing*, pages 461–464, 2011.

[7] ERTMS Benefits. http://www.ertms.net/?page_id=44. Acc.: 2019-02.

[8] Capacity for Rail (C4R). *Operational failure modes of Switches and Crossings*. C4R, 2015. Public deliverable–'D1.3.1'.

[9] J. Sramota and A. Skavhaug. RailCheck: A WSN-Based System for Condition Monitoring of Railway Infrastructure. In *21st Euromicro Conference on Digital System Design (DSD)*, pages 347–351, 2018.

[10] IEC 60812:2018 - Failure modes and effects analysis (FMEA and FMECA). https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=988328. Accessed: 2019-02-04.

[11] Material Data sheet - PA2200. http://www.shapeways.com/topics/udesign/materials/white_strong_flexible/pa2200_material_data_sheet_12_08_en__.pdf. Accessed: 2019-02-04.

[12] ISO 179-1:2010 – Plastics - Determination of Charpy impact properties. http://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=432313. Accessed: 2019-01-30.

[13] IEC 60529:1989 – Degrees of protection provided by enclosures (IP Code). http://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=658451. Accessed: 2019-01-30.

[14] CENELEC. EN 50159:2010 – Safety-related communication in transmission systems. *Official Journal of the European Union*, 2010.

[15] BaneNOR. Signal/Prosjektering/Sporveksel og sporsperreutrustning. https://trv.banenor.no/wiki/Signal/Prosjektering/Sporveksel-_og_sporsperreutrustning#RAMS_-_krav. Accessed: 2019-03-05.

[16] NSW. TMC227-Surface Defects in Rails. https://www.transport.nsw.gov.au/system/files/media/asa_standards/2017/tmc-227.pdf. Acc: 2019.

[17] SKF. Bogie condition monitoring – Extract from the Railway technical handbook, volume 1, chapter 8, page 152 to 163. https://www.skf.com/binary/12-62755/RTB-1-08-Bogie/index.html. Accessed: 2019-04-02.