Cyclisation of Safety Diagnoses: Influence on the Evaluation of Fault Metrics

Armin Köhler, Robert Bosch GmbH

Bernd Bertsche, Prof. Dr.-Ing., University of Stuttgart

Key Words: Automated Driving, Diagnostic Coverage, Functional Safety, ISO 26262, PMHF, Powernet, Safety Measures

SUMMARY & CONCLUSIONS

This technical elaboration derives a new mathematical approach for Probabilistic Metric for random Hardware Failures (PMHF) calculation of intended functionalities that relate to cyclic safety measures with Diagnostic Coverage (DC). Thereby the probability density function of exponential failure distribution is adapted to the cyclic influence of safety diagnosis. All time dependent safety aspects of the system behavior are considered. That results in a piecewise density function, which is approximated for integration as a cumulative distribution function. This leads to a new definition of a cyclic DC rate and PMHF calculation. In addition to that, an appropriate FTA model will be described. Thereby, some current approaches of PMHF calculation are proven as incorrect for the target use case. Analysis and comparisons with state of the art will show the normative and engineering benefit of the concept. For example: a time discrete approach of the defined cyclic DC calculation method can be applied to predictive diagnostics and system state forecasting functions that are used in autonomous driving vehicles. This faces especially future vehicle applications. The new methodology will be illustrated with examples out of the area of vehicle powernet and safety diagnoses. The results of this investigation will be very valuable for safety engineers and auditors dealing with technical systems and implemented safety measures.

ORGANIZATION OF THE ARTICLE

Starting with the introduction of the general topic in section 1, the issues and objectives of the elaboration are given. The background information about vehicle powernet and basic information about safety measures are introduced as well as the related key points of the ISO 26262 safety validation process. Fundamental definitions of reliability engineering are stated in section 2. Based on this, the technical safety measure itself and its diagnostic functionality is introduced in section 3. The scope and underlying assumptions of the investigation are defined. In Section 4, the state-of-the-art approaches are introduced and discussed. After that, the novel approach for cyclic safety measures is elaborated and derived in detail which ends up in a FTA model assumption. In the last section 6, the results of all mentioned approaches are discussed and evaluated extensively using theoretical and graphical analyses. The accomplished engineering benefits of the novel approach are pointed out.

1 INTRODUCTION

Driven by the global megatrends such as electrification and automation, the automotive sector highly expands into technical and innovative domains. Especially the working area of Advanced Driver Assistance Systems and automated driving technologies is a current field of innovations. Most of these systems share a same characteristic: they belong to electrical and/or electronic (E/E) systems, which are responsible for the safety of drivers and passengers. Thereby, the basis of functionality is always the sufficient power supply of these safety related systems and therefore it is inevitable. As a result, the safety relevance of powernets and related components rise enormously. For this reason, the whole powernet has to be developed and verified according to functional safety standards. Especially in the sector of road vehicles, the functional safety process according to ISO 26262 has to be applied.

The current development process of powernets is limited to the analysis of voltage stability and load balance. Future powernet developments additionally need to consider legislation, safety, technical standards – especially ISO 26262 – and reliability. Thus, various technical measures are getting inevitable on powernet level like intelligent switching modules or predictive system diagnoses. In the ISO 26262, an extensive safety analysis is claimed for these kind of safety systems. Therefore, the quantitative evaluation is particularly based on the calculation of the Probabilistic Metric for random Hardware Failures (PMHF). The metric value PMHF is under wide influence of the implemented safety diagnoses or safety measures due to their Diagnostic Coverage (DC) rates.

Presently the common understanding is that the DC can have a positive influence on the PMHF of a safety related functionality. On the contrary, the explicit way the diagnosis influences the metric values is not obvious. In science, research and everyday business, there are different understandings and calculation methods with huge variations on the metric values. Some of these methods are often used under wrong conditions. In addition to that, most of current technical safety measures operate in a time discrete mode due to sample rate and cyclisation (e.g. self-check or calibration at power up/down phase). That property is not considered for calculation nowadays. To be more specific, there are three major open

978-1-7281-8017-5/21/$31.00 ©2021 IEEE

points regarding this kind of safety analysis:

- the time dependent influence of cyclic diagnoses,
- the related mathematical model,
- the modelling in a Fault Tree Analysis (FTA) [1].

Current approaches do have significant differences in most of their criteria. Furthermore, none of these approaches considers cyclic DC. It is necessary to reinvent the approach from bottom up beginning with general definitions.

1.1 *Objective*

This paper derives a novel calculation and modelling approach for cyclic safety measures. This is done in accordance with the normative foundations of the ISO 26262 standard. The purpose of this investigation is to enhance the safety validation process from continuous diagnostic functions to a general time dependent methodology. The time dependent influences and the mathematical model of the novel approach are elaborated, as well as an appropriate FTA is given. Various current methods are introduced, discussed and compared to each other.

1.2 *Background Information: Vehicle Powernet*

A system engineering process for safe power supplied vehicles initiated the investigation of the methodology described in this paper. With that background and for the reason of better illustration, some points of this elaboration refer to exemplary topics and examples out of the area of powernet. A schematically approach of a vehicle powernet architecture is illustrated in Figure 1 [2]. This section gives a brief overview about the most relevant subjects.

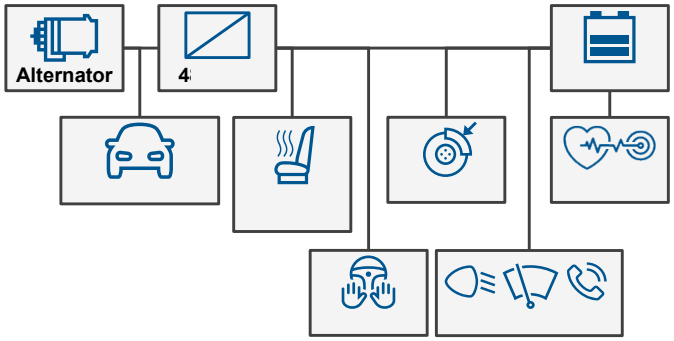

Figure 1 – Schematically Powernet Architecture

With automated driving functionalities and Advanced Driver Assistance Systems implemented in the vehicle, the safety requirements for component power supply are significantly changing [2]. Giving a simple example to underline that fact: An Electronic Power Steering actuator requires a specific load profile to perform as requested. In case the power supply is not able to deliver that load profile, e.g. due to a short circuit to ground or non-performant battery, a hazardous event could occur. The 12 V battery is a well-known component with high potential of having a fault in either power distribution or power supply. To be more specific, battery faults leading to a powernet breakdown could be:

- discharged / aged / cold / non-performant battery,
- false battery type,
- (cell) short circuit / open circuit of battery.

In order to fulfill the safety requirements on powernet level and detect or control the battery faults, technical Safety Measures (SM) have to be implemented [3]. This could be an Electronic Battery Sensor (EBS) for example, which ensures smart battery monitoring and pre-detection of faults.

Giving a theoretical example: The prognostics and health management of the battery often uses the internal resistance R_i of the battery as an essential value. The determination of R_i has one major constraint: it is based on the temporal change of voltage and current:

$$R_i = \Delta U / \Delta I \ . \qquad (1)$$

For an accurate measurement, a pulse with high peak values works fine. Usually this battery stimulation is given due to the engine start up pulse. This can be quite a few of hundreds of amperes. After the engine is started once, there is no more comparable pulse like this anymore. Because of a zero-current operating strategy of the battery, there is often no more battery pulse at all in the drive cycle. Nevertheless, a sufficient R_i monitoring of the battery is required due to mandatory standards like ISO 26262. The only solution in this case would be a frequent active stimulation of the battery. This could be done by a forced turn on of high-power consumptive loads, e.g. seat heating or windshield heating. Due to power consumption or comfort constraints, this is obviously not a feasible approach.

The given example of battery monitoring underlined that in general, some diagnostic functions or safety measures can only perform in a time discrete or cyclic manner and not continuous. This can have several reasons like:

- unavailability of required system states,
- operating strategy or physical constraints,
- sampling rate of electronic components,
- non-real-time communication interface,
- vehicle bus overload and data loss,
- long lasting and time dependent calculation methods (e.g. Kalman filtering),
- computing resources.

Those kind of diagnoses or safety measures, which have a significant influence of cyclisation, must not be treated as continuous systems in the safety validation process.

1.3 *Safety Validation Process according to ISO 26262*

For vehicle systems with an Automotive Safety Integrity Level (ASIL) down to ASIL-A, evidence of the effectiveness of implemented safety measures shall be made available. This affects safety measures, which are applied to prevent faults from leading to Single Point Faults (SPFs) or to reduce Residual Faults (RFs). If the Fault Handling Time Interval (FHTI) of the safety measure is greater than the Fault Tolerant Time Interval (FTTI), the safety measure must not be considered as being effective and therefore it cannot be taken into account for the safety validation. Thereby the FHTI contains the Diagnostic Test Time Interval (DTTI), which is the limiting factor due to cyclisation effects (see Fig. 2) [4,5].

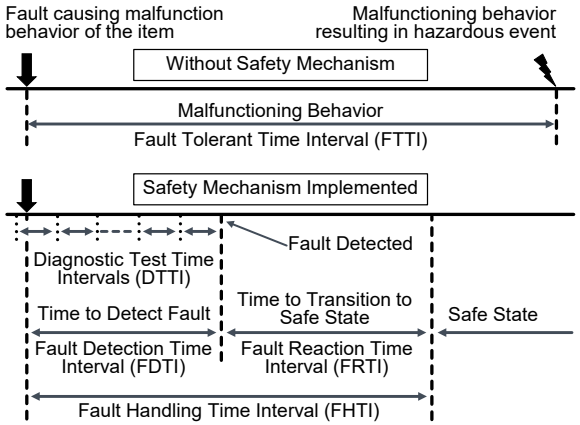

Figure 2 – Time Intervals

Referring to the example of battery monitoring, the Safety Goal (SG) could be: Avoid the sudden loss of steering assist due to non-performant battery. A loss of steering function could be rated as acceptable if it does not occur for longer than 100 ms. Therefore, the FTTI for this safety goal is 100 ms. That means that the dedicated safety measure, including the battery monitoring for the detection of the specific fault, has to perform within the FTTI of 100 ms. As mentioned in section 1.2 this could be not feasible under usual conditions.

Generally speaking: Safety measures, which are under influence of cyclisation, potentially violate the criteria FHTI ≤ FTTI. According to the safety validation process of ISO 26262, these safety measures must not be taken into account for validation of related SPFs and RFs due to systematic fault influence. In order to change that, a novel approach for safety validation process of safety measures with FHTI ≥ FTTI is described in this paper.

2 FUNDAMENTAL DEFINITIONS

The derivation of the novel methodology is based on fundamental definitions. The bottom-up investigation is initiated with the following definitions.

2.1 *Failure Types*

A Single-Point Fault (SPF) is a fault in an element that leads directly to the violation of the safety goal. No fault of the related element is covered by any safety mechanism [5].

A Latent Fault (LF) is a Multiple-Point Fault (MPF) which is not detected by any safety mechanism nor perceived by the driver within the multiple-point fault detection time interval [5].

A Residual Fault (RF) is the portion of random hardware faults that by itself lead to a violation of the safety goal. This portion is not controlled by any safety mechanism. The remaining portion of faults of the hardware element is controlled by a safety mechanism in contrary to a SPF [5].

A dormant SPF/RF is a fault that causes an error only under particular conditions [6]. The violation of the safety goal emerges only under particular operating status. E.g. if the battery has a decreased capacity a violation of the safety goal will only occur in particular driving situation. This could be for example a high-power consumption of base loads with an instant evasive maneuver in parallel.

2.2 *Failure Distribution Function*

Random hardware faults of E/E systems are determined according to the exponential distribution. According to ISO 26262 these systems are non-repairable. Thereby the failure rate λ is considered as constant [7]. The unit of λ is Failure In Time (FIT) which is the number of failures in 10^9 device-hours of operation. The related probability density function is:

$$f(t) = \lambda \cdot e^{-\lambda \cdot t} . \quad (2)$$

The related cumulative distribution function is given as:

$$F(t) = \int f(t) = 1 - e^{-\lambda \cdot t} . \quad (3)$$

The distribution function corresponds to the histogram of the cumulative frequency and provides insight into quantity of faults until the observed point of time. The distribution function always has its beginning at $F(t) = 0$ and a steady state at $F(t) = 1$. It is a monotonic increasing function [8].

2.3 *Diagnostic Coverage (DC)*

The Diagnostic Coverage (DC) is the percentage of the failure rate λ of a hardware element or failure mode that is detected or controlled by an implemented safety mechanism:

$$DC = \lambda_{dd}/\lambda_d = \lambda_{dd}/(\lambda_{dd} + \lambda_{du}) . \quad (4)$$

with the failure rate proportion of dangerous λ_d, dangerous-detected λ_{dd} and dangerous-undetected λ_{du} faults. Note: By definition, the DC is associated with the failure rate, not the failure distribution [5,9].

2.4 *Probabilistic Metric for random Hardware Failures*

One of the most relevant Metric values is the Probabilistic Metric for random Hardware Failures (PMHF). It is defined as the average probability per hour over the operational lifetime T_L (see Eq. 5).

$$PMHF = \frac{Prob(T \le T_L)}{T_L} = \frac{\int_0^{T_L} f(\tau) \cdot d\tau}{T_L} = \frac{F(t)\,|_{t=T_L}}{T_L} . \quad (5)$$

The operational lifetime only includes operating hours. The unit of the PMHF is FIT as well as it is of the failure rate λ. Nevertheless, PMHF and λ are completely different values with different meanings [4,7]. The intentions of $F(t)$, $f(t)$ and the PMHF are visualized in Figure 3 [7].

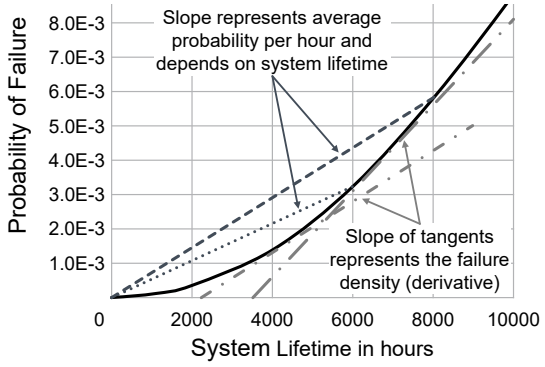

Figure 3 – Visualization of PMHF

3 TECHNICAL SAFETY MEASURES

Technical safety measures are solutions to detect or control random hardware failures or mitigate their harmful effects. On the other hand, a safety mechanism is the technical solution implemented by E/E functions to detect, mitigate or tolerate faults as well as control or avoid failures. By that, the intended functionality is maintained, or the safe state achieved. Safety measures include safety mechanisms.

3.1 *Diagnostic Function of Safety Measures*

The way, a safety measure influences the system is described using a theoretical example. Assumption: A system with the possibility of random hardware faults that lead to a hazardous event is controlled by a safety measure. This safety measure is able to detect and control all occurring failure modes. The failure rate of all combined potential failures is constant with $\lambda = 10\ FIT$. The safety mechanism of the safety measure transitions the system into the safe state within the FTTI. Thereby the diagnostic coverage is 100 %. The safety measure and its diagnostic function is only activated in one time interval. Figure 4 is the demonstration of the given example.

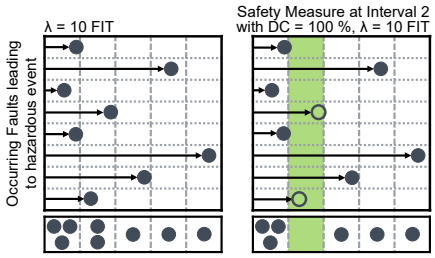

Figure 4 – General Effect of Safety Measures

The diagram on the left is the representation of the system without safety measure, the one on the right with a safety measure effecting interval two. Due to the safety measure with *DC = 100 %*, there are no remaining faults in interval two anymore. The empirical density and the corresponding distribution of failures (see Fig. 5) represent the remaining faults of each time interval. The failure distribution is stagnating in the controlled interval and thus the failure distribution value decreases for the further timer intervals in comparison to the non-controlled system. With the definition of the DC, the failure rate λ at interval 2 with safety measure is:

$$\lambda_{Int.2,SM} = \lambda \cdot (1 - DC) = 10\ FIT \cdot (1 - 100\ \%) = 0\,. \quad (6)$$

As a result, the safety measure effects the failure rate λ, the failure density *f(t)* and the failure distribution *F(t)* depending on the controlled time interval and the DC rate.

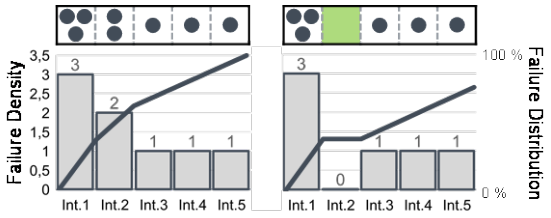

Figure 5 – Mathematical Effect of Safety Measures

3.2 *Scope of the Investigation*

The way safety measures effect the underlying process highly depends on the specific boundary conditions. E.g. the modelling of a latent multiple point fault differs from the modelling of a SPF. For this paper investigations and all related approaches, the boundary conditions are:

- all faults are random hardware faults (not systematic),
- scope of the safety measure are RFs and dormant SPFs,
- the system is non-repairable with λ = *const.*,
- the PMHF corresponds to the probability of failure *F(t)*.

As stated in the IEC 61508, safety related systems at the highest safety level (e.g. faults directly leading to the violation of safety goal) must be modelled using the unreliability *F(t)*. Systems, which are on a lower safety level (e.g. multiple point faults) can be modelled using the unavailability *Q(t)*. The unreliability represents the probability of failure within a defined time interval. In comparison to that, the unavailability represents the probability of failure at a specific point of time. For an observed system the unavailability has a sawtooth-shaped behavior, the unreliability is still monotonic increasing [1,9,10].

Even if these assumptions are restrictive, they represent a common use case configuration. This enables the possibility of a use case adaption of the methodologies to differing boundary conditions. It is expectable that the application of the approaches could change, but not the methodology in principle.

4 STATE OF THE ART APPROACHES

The current approaches for the modelling of safety measures with DC rate are validated in this section. The comparison of all approaches is given in section 6.

4.1 *ISO 26262 Approach*

The ISO 26262 gives a clear definition about the modelling of safety measures. In context to the definition of the DC, the failure distribution and the PMHF are defined as:

$$PMHF = \frac{F(T_L)}{T_L} = \frac{1 - e^{-(1-DC)\cdot\lambda\cdot T_L}}{T_L} \approx \frac{(1 - DC)\cdot\lambda\cdot T_L}{T_L}\,. \quad (7)$$

This approach is only valid for continuous safety measures with FHTI ≤ FTTI (→ static safety measure); no cyclisation is taken into account. The calculation within the FTA is not explicitly mentioned but can be achieved with a pre-calculated failure rate $\lambda_{new} = (1 - DC)\cdot\lambda$ as a base-event [4,7].

4.2 *Best Practice Approach*

A well-known approach of functional safety experts gives the FTA modelling with the DC value as a several base-event: $\{\lambda \wedge \overline{DC}\}$. This is very valuable, because this FTA is more manageable and dynamic. The mathematical model leads to:

$$PMHF = F(T_L)/T_L = (1 - DC)\cdot\left(1 - e^{-\lambda\cdot T_L}\right)/T_L\,. \quad (8)$$

Referring to this derived formula, the main trade-off is revealed: the steady state of the failure distribution is $F(t \to \infty) = (1 - DC)$ and not as it is defined $F(t \to \infty) = 1$. This is a non-conservative approximation into unsafe direction. This approach is only ISO 26262 conform with certain conditions ($\lambda t \ll 1$). In addition, this approach is only valid for

static safety measures with FHTI ≤ FTTI as well.

4.3 *Unavailability Approach*

Another approach faces the cyclic effect due to a dormant (sawtooth-shaped) base event modelling as *Q(t)*. The frequency is set to the diagnostic period of time T_{Diag} (e.g. 1 drive cycle = 1 h). With $Q(t) \triangleq F(t)$, the maximum value of PMHF is:

$$PMHF = F(T_{Diag})/T_L = (1 - e^{-\lambda \cdot T_{Diag}})/T_L \ . \quad (9)$$

The PMHF value will be low in comparison to the ISO 26262 approach and can vary in several orders of magnitude. As described in section 3.2, the modelling of RFs and dormant SPFs has to be done according to *F(t)*, not *Q(t)*. For this reason, this approach is not valid. Even if the cyclisation is taken into account, the DC is not, and it is assumed to be *DC = 100 %*.

4.4 *Splitting F(t) Approach*

A recent internal study came up with a solution taking cyclisation and DC rate into account. Therefore, the DC is distributed into DC_{static} and DC_{cyclic}. It is assumed, that the system can only be controlled in a proportion of the safety measure period T_{Diag}, due to cyclisation. This proportion is represented with the cyclic DC:

$$DC_{cycl} = t_{controlled}/T_{Diag} \ . \quad (10)$$

The DC_{static} still represents the usual effectiveness of the safety measure in case it is in a continuous manner. The DC_{static} effects the whole time interval $T_{Diag} = t_c + t_d$, whereas the dangerous proportion adds extra failure probability with DC_{cycl}. The FTA model is realized as: $\{(\lambda \wedge \overline{DC_{stat}}) \vee (\lambda \wedge DC_{stat} \wedge \overline{DC_{cycl}})\}$. This complies with the formula:

$$PMHF = F(T_L)/T_L = (F(T_L)_{stat} + F(T_L)_{cycl})/T_L$$
$$= \frac{(1\text{-}DC_{stat})(1\text{-}e^{-\lambda \cdot T_L}) + DC_{stat}(1\text{-}DC_{cycl})(1\text{-}e^{-\lambda \cdot T_L})}{T_L} \ . \quad (11)$$

Even if this approach is valid for cyclic safety measures with different DC values, the steady state value of $F(t \to \infty) = (1 - DC_{stat} \cdot DC_{cycl})$ does not comply to the definition.

5 *NOVEL APPROACH FOR CYCLIC DIAGNOSES*

The investigation of the novel approach for cyclic diagnoses bases on elementary time sequences and fundamental definitions.

5.1 *Time Dependencies of Diagnoses*

According to ISO 26262 [4,7] all time dependencies that relate to cyclic diagnoses are derived into detail (see Fig. 6). The cyclic Safety Measure (SM) with a period of T_{Diag} is divided in its subsequences. The absolute time value of the period T_{Diag} is intended as "safety measure completed", so at the end of the FHTI. The FHTI itself consists of the FDTI and FRTI, whereby the FDTI has multiple underlying DTTI (cf. Fig. 2). With the new definition of the Cause Effect Time Interval (CETI), the malfunction behavior is divided in its inherent time dependencies as well. The root cause is the failure initiating event which emerges after the CETI as an error. This error is acceptable on system level for the duration of the defined FTTI. After exceeding this threshold, the hazardous event (fault or safety goal violation) occurs.

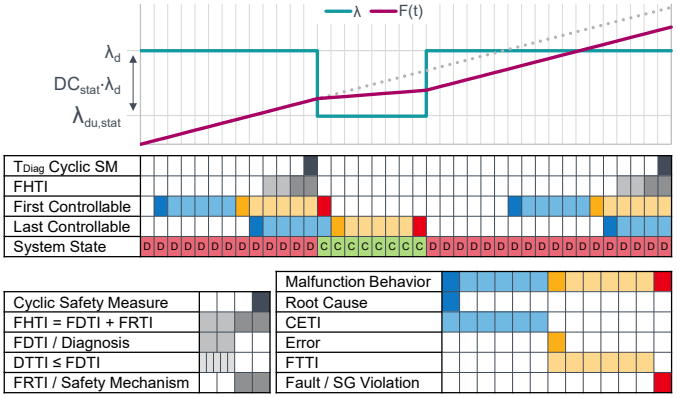

Figure 6 – Timing Diagram of Cyclic Fault Behavior

Doing this, the first and last potential faults that can even be controlled with the safety measure are identified (root cause detection). The system state thereby is stated as controlled t_c. Whilst the controlled system state, the failure rate of the system decreases from its initial value λ_d to $\lambda_{du,stat} = (1 - DC_{stat}) \cdot \lambda_d$, with $DC_{stat} = \lambda_{dd,stat}/\lambda_d$ represented by the piecewise failure rate function (cyan line):

$$\lambda = \begin{cases} \lambda_{du,stat} \ , & \text{if } t \in t_C \\ \lambda_d \ , & \text{if } t \in t_D \end{cases} \ . \quad (12)$$

This leads to a cumulative failure distribution function $F(t) = \int f(\lambda, t)\, dt$ (purple line) with a decreased slope in the controlled period. This relation of *F(t)* and controlled system states reflects the positive influence of cyclic safety measure. With decreasing FHTI and T_{Diag}, the effectiveness of the safety measure and the controlled time interval t_c increases. The safety measure converges back to static (continuously) behavior.

5.2 *Cyclic Diagnostic Coverage: f(t)-mean*

With the given relations of T_{Diag}, *f(t)* and *F(t)* the mathematical model is established. With the alternating failure rate depending on t_C and t_D, the failure density is modelled as a piecewise density function:

$$f(t)_{cycl} = \begin{cases} \lambda_{du,stat} \cdot e^{-\lambda_{du,stat} \cdot t} \ , & \text{if } t \in t_C \\ \lambda_d \cdot e^{-\lambda_d \cdot t} \ , & \text{if } t \in t_D \end{cases} \ . \quad (13)$$

With the definition of the cyclic factor $K_C = t_C/(t_C + t_D)$, the weighted average of the piecewise density is given as:

$$f(t)_{cycl} = K_C \cdot \lambda_{du,stat} \cdot e^{-\lambda_{du,stat} \cdot t} + (1 - K_C) \cdot \lambda_d \cdot e^{-\lambda_d \cdot t} \ . \quad (14)$$

The related distribution function is:

$$F(t)_{cycl} = K_C \cdot (1 - e^{-\lambda_{du,stat} \cdot t}) + (1 - K_C) \cdot (1 - e^{-\lambda_d \cdot t}) \ . \quad (15)$$

The related PMHF by that is: $PMHF = F(T_L)_{cycl}/T_L$. An FTA model approach could be the combination of pre-calculated failure rates and coefficients $\{(\lambda_{du,stat} \wedge K_C) \vee (\lambda_d \wedge \overline{K_C})\}$ with an underlying influence of DC_{stat} (see Fig. 7).

This approach complies with the theoretical values and

matches the simulation described in section 6.

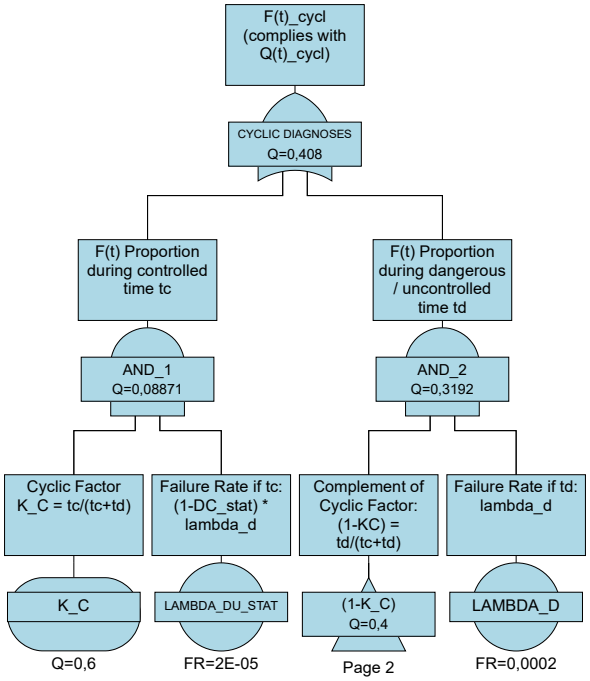

Figure 7 – FTA Approach of $F(t)_{cycl}$

6 COMPARISON AND RESULTS

The graphical comparison of all mentioned approaches is presented in Figure 8. The simulation parameters are: $\lambda = 200\ E{+}3\ FIT$, $DC = DC_{stat} = 90\ \%$, $K_C = 0.6$ and $T_L = 8000\ h$. These values are theoretical examples, which could represent the behavior of a lead acid battery with a supervised safety measure, depending on the specific use case. For the reason of a clear illustration, the diagnostic period T_{Diag} is set to 200 h. The theoretical comparison is described in Table 1.

The probability of failure of the system without any safety measure is represented by the black distribution function $F(t)_{total}$. The distribution functions $F(t)$ of "ISO 26262" (cf. Eq. 7) and "Best Practice" (cf. Eq. 8) approach are only representative for a static system. The cyclic parameter K_C has absolutely no effect on the calculation and a cyclic system is improperly treated as a continuous system. As a result, these approaches deliver too optimistic and non-conservative $F(t)$ or PMHF values for cyclic diagnoses with FHTI ≥ FTTI. Therefore, these approaches are not valid for- or comparable to such cyclic diagnoses. Also the "Unavailability" approach (cf. Eq. 9) is not comparable because the unavailability $Q(t)$ does not address RFs or SPFs. The "Splitting" approach (cf. Eq. 11) seems to be very likely, but it does not comply with the steady state definition of $F(t)$. If $\lambda t \ll 1$ is not valid, the approach delivers non-conservative results.

The novel "$F(t)_{cyclic}$" approach (in green) with the weighted average $f(t)_{cyclic}$ (dashed green) of the piecewise density function $f(t)_{piecewise}$ (in grey) complies with the steady sate definition, and cyclic effects, even if FHTI ≥ FTTI. The described model also complies with the ISO 26262 definitions and expands the standard method of continuous diagnoses to an adaptable and general approach for static or cyclic safety measures. State of the art approaches do not allow the modelling of these kind of system behavior as a constraint of ISO 26262. By contrast, the safety system itself or hardware functions would need to be redesigned (e.g. redundancies or proper hardware elements) in order to reduce the $F(t)$ and PMHF values. On the other hand, a reduction of the system probability of failure $F(t)_{total}$ with $\Delta F(t)$ could be reached, when the novel approach is applied to the implemented safety system. In addition to that, the PMHF value decreases, which leads to a positive influence on the safety validation process as well.

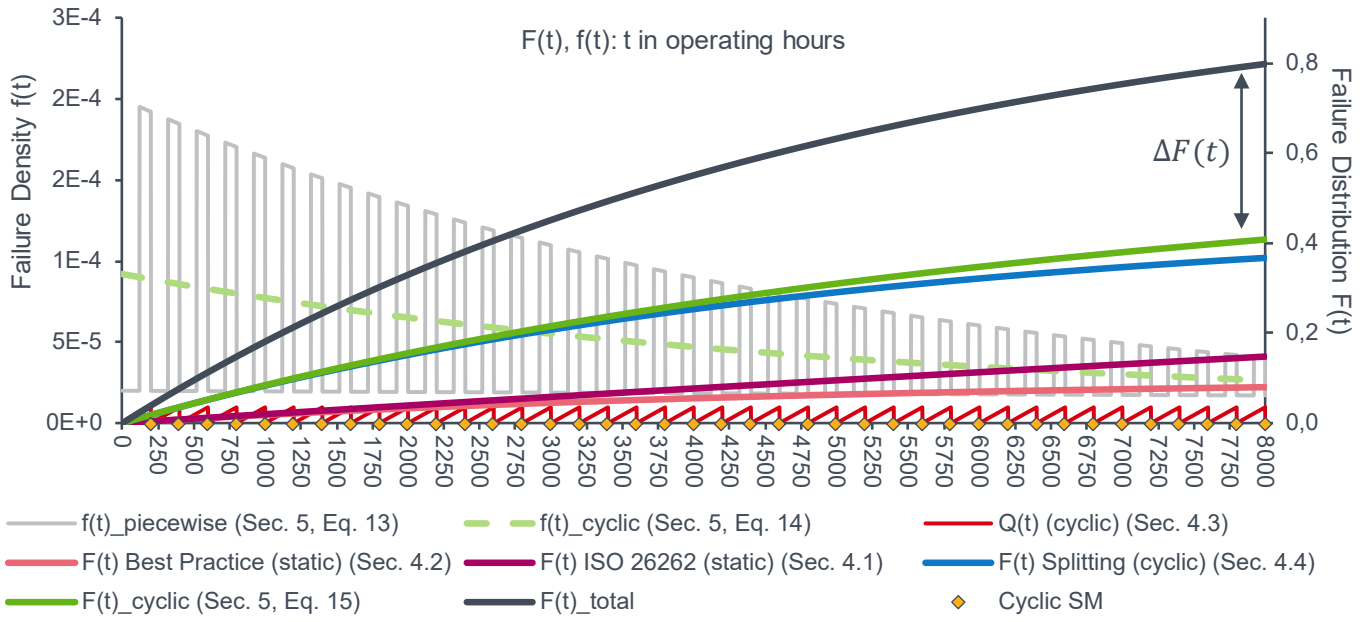

Figure 8 – Graphical Approach Comparison

Table 1 – Approach Comparison

Criteria	ISO 26262	Best Practice	Unavailability	Splitting	F(t)_cyclic / f(t)-mean
Short Description	λ Correction	F(t) Coefficient	Sawtooth-Shaped Model	F(t) Splitting	f(t) Density Mean
Model Parameter	F(t)	F(t)	Q(t) ≙ F(t)	F(t)	F(t)
Parameter Influence	DC	DC	SM Time Period T_{Diag}	DC_{stat}, $DC_{cycl} = t_c/(t_C + t_D)$	K_C, DC_{stat}
Time Dependency	Static	Static	Cyclic	Static, Cyclic	Static, Cyclic
Mathematic Model $F(t) = \ldots$	$1 - e^{-(1-DC)\cdot\lambda\cdot t}$	$(1 - DC) \cdot \left(1 - e^{-\lambda\cdot t}\right)$	$1 - e^{-\lambda\cdot T_{Diag}}$	$(1\text{-}DC_{stat})\left(1\text{-}e^{-\lambda\cdot T_L}\right) + DC_{stat}\left(1\text{-}DC_{cycl}\right)\left(1\text{-}e^{-\lambda\cdot T_L}\right)$	$K_C \cdot \left(1 - e^{-\lambda_{du,stat}\cdot t}\right) + (1 - K_C) \cdot \left(1 - e^{-\lambda_d\cdot t}\right)$
Steady State $F(t \to \infty) = \ldots$	1	$(1 - DC)$	$1 - e^{-\lambda\cdot T_{Diag}}$, $F\left(T_{Diag} \to \infty\right) = 1$	$1 - \left(DC_{stat} \cdot DC_{cycl}\right)$	1
FTA Model	$\{(1 - DC) \cdot \lambda\}$	$\{\lambda \wedge \overline{DC}\}$	$\left\{\lambda_{dormant(T_{Diag})}\right\}$	$\{(\lambda \wedge \overline{DC_{stat}}) \vee (\lambda \wedge DC_{stat} \wedge \overline{DC_{cycl}})\}$	$\{(\lambda_{du,stat} \wedge K_C) \vee (\lambda_d \wedge \overline{K_C})\}$
Constraint	$FHTI \leq FTTI$	$FHTI \leq FTTI$	$DC = 100\,\%$	-	-
Additional Information	Static Reference	Conform to Approximation of ISO 26262 Approach	Not valid for RF/SPF	Non-conservative if $\lambda t \ll 1$ is not valid	Approach not yet confirmed

REFERENCES

1. F. Edler, M. Soden, R. Hankammer, „Fehlerbaumanalyse in Theorie und Praxis," München/Berlin: Springer, 2015.
2. A. Köhler, B. Bertsche, "An Approach of Fail Operational Power Supply for Next Generation Vehicle Powernet Architectures," (in prep.).
3. ISO 26262, "Road vehicles - Functional safety –," 2018.
4. ISO 26262-5:2018-12, "Road vehicles – Functional safety – Part 5: Product development at the hardware level," 2018.
5. ISO 26262-1:2018-12, "Road vehicles – Functional safety – Part 1: Vocabulary," 2018.
6. IEC,"Electropedia," Available: http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=192-04-07. [Accessed Jul. 15 2020].
7. ISO 26262-10:2018-12, "Road vehicles – Functional safety – Part 10: Guidelines on ISO 26262," 2018.
8. B. Bertsche, "Reliability in Automotive and Mechanical Engineering," Berlin: Springer, 2008.
9. IEC 61508-4:2010-12 "Functional safety of electrical/ electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations," 2010.
10. A. Birolini, "Reliability Engineering – Theory and Practice," Zurich/Florence: Springer, 2017.

BIOGRAPHIES

Armin Köhler
Automotive Electronics, Product Area Energy Management
Powernet - Architecture (AE-BE/PAN2)
Robert Bosch GmbH
Mittlerer Pfad 9
70499 Stuttgart, Germany

e-mail: Armin.Koehler3@de.bosch.com

Armin Köhler studied Electrical Engineering at the Karlsruhe University of Applied Sciences and earned his academic degree Master of Science in 2018. He is working as a doctoral student in the field of functional safety in the area of automotive electronics – powernet. He is pursuing his PhD studies with a focus on technical safety measures in cooperation with the Reliability Engineering Department, Institute of Machine Components, University of Stuttgart.

Bernd Bertsche, Prof. Dr.-Ing.
Institute of Machine Components
University of Stuttgart
Pfaffenwaldring 9
70569 Stuttgart, Germany

e-mail: bernd.bertsche@ima.uni-stuttgart.de

Bernd Bertsche began his professional career at Daimler AG in Stuttgart from 1989-1992. He has been a Professor of Mechanical Engineering at the Institute of Machine Components at the University of Stuttgart, as well as the Head of the Reliability Engineering Department since 1996. In 2001 he became Head of the Institute, as well as Head of the VDI Advisory Board "Reliability Management". Since 2003 he has been member of the DIN/DKE Standardization Committee K132 "Reliability". He was elected to be a member of the review board of the German Research Foundation in 2012. 2013 he was elected to be the managing director of the WiGeP e.V. As of 2015 he has been a member of the National Academy of Science and Engineering.