A fault-tolerant control architecture for different battery topologies in electric vehicles

Gholami, Mehdi; Esen, Hasan; Schiøler, Henrik; Stoustrup, Jakob

Published in:
8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes

DOI (link to publication from Publisher):
10.3182/20120829-3-MX-2028.00251

Publication date:
2012

Document Version
Early version, also known as pre-print

A Fault-Tolerant Control Architecture for Different Battery Topologies in Electrified Vehicles

Mehdi Gholami * **Hasan Esen** ** **Henrik Schioler** *** **Jakob Stoustrup** ****

* *Aalborg University, Fredrik Bajersvej 7C, 9220, Aalborg, Denmark (e-mail: mg@es.aau.dk).*
** *DENSO AUTOMOTIVE Deutschland GmbH, Freisinger Str. 21, 85386 Eching, Germany (h.esen@denso-auto.de)*
*** *Aalborg University, Fredrik Bajersvej 7C, 9220, Aalborg, Denmark (e-mail: henrik@es.aau.dk).*
**** *Aalborg University, Fredrik Bajersvej 7C, 9220, Aalborg, Denmark (e-mail: jakob@es.aau.dk).*

Abstract: In this paper a variety of battery configuration topologies for electrified vehicles are investigated with regard to reliability and expected lifetime along with the possibility of applying active fault detection to provide early warnings for the driver. Different configurations are investigated ranging from a simple single serial string of battery cells providing only the lowest level of fault tolerance, to a highly elaborate and still practically relevant triple string configuration providing fault detection and reconfiguration possibilities as well as repair. All configurations are analyzed with regard to the associated reliability profile assuming non-ageing cell failure model. A novel method for active early fault detection is presented based on encoding faults into a parametric dynamic cell model, where parameters are continuously estimated under the influence of an auxiliary test signal designed to optimize parametric sensitivity. Finally reliability profiles for all investigated configurations are compared mutually and with standard requirements on the basis of mean time to failure statistics.

Keywords: electrical vehicles, fault tolerance, fault detection, battery configuration, reliability analysis

1. INTRODUCTION

One of the most important fields of safety critical systems is the transportation, including air-, train-, ship- and road-transport. Whereas the former is normally considered the field of highest safety criticality due to the high risk of fatalities following failure in flight, the latter is of no less importance due to the mere volume of vehicles. The number of road accident fatalities per year by far outweighs that of air traffic, which is often forgotten in the public debate. Only a fraction of road accidents are caused by equipment failure, but considering the volume of traffic, even small improvements of equipment reliability heavily impacts statistics of injury and death in terms of absolute numbers. Electrical and hybrid vehicles (EHV) have been commercially available for a decade, however challenges from oil supply shortage and environmental protection the expected market share of EHV is expected to rise dramatically over the decade to come. In this light, special attention to the safety engineering of such vehicles and their components becomes highly appropriate. In this paper we investigate reliability and fault tolerance issues associated to the battery component of EHVs and its management.

The litterature on fault tolerance on EV batteries is still sparse although few examples are to be found. For example, authors in Hagen et al. (2000) and Weng (2009) propose a fault tolerant methodology, where a battery computer monitors different battery conditions such as the voltage and current state of the battery, and applies over-discharge protection system, equalization and adjustment to protect the battery. In Laidig and Wurst (2006), a data history of the impedance of the battery is acquired and examined to predict occurrence of future fault. The authors of Bhangu et al. (2005) use Kalman filter (KF) to estimate a parameter of the EV battery model and distinguish state of health (SoH) of the battery. In Chatzakis et al. (2003), Affanni et al. (2005) and Stuart et al. (2002), a series battery configuration is suggested and an electric circuit to protect the batteries from short circuit and other failure is designed.

In this paper, we examine different battery configuration for HEVs and investigate safety of each configuration with respect to reliability and mean time to failure (MTTF), hereafter an early fault detection algorithm to warn the driver in advance and in turn increase safety is designed. The suggested detection method belongs to the category of active fault detection schemes and is similar to what is proposed in Gholami et al. (2011b). In general fault

detection is divided into passive or active methods. The passive ones observe corresponding input/output signals of the system to detect the fault, see Anwar (2010), while the active ones excite the system to detect faults hidden under normal operation or to detect faults faster, see Gholami et al. (2011a). By comparing the reliability and MTTF of each configuration we demonstrate that early fault detection improves the safety of the battery configurations.

The organization of the paper is as follows: Section 2 presents different battery configurations. Design of early fault detection is discussed in Section 3. Section 4 is dedicated to reliability and MTTF assessment of different configurations. Section 5 describes the reliability improvement by early fault detection mechanism. Finally the conclusion is presented in Section 6.

2. BATTERY CONFIGURATIONS

The battery pack constitutes a major part of the energy supply in HEVs, and in case of a battery electric vehicle (BEV), it is the only energy source. It is most often composed by a number of individual low voltage cells in a fixed configuration, designed to fit the voltage and current requirements of the vehicle. Following the examples, we can outline 3 main battery topologies: (A)single serial string (B)2 parallel strings, and (C) multiple parallel strings. Example topologies are shown in Fig. 1.

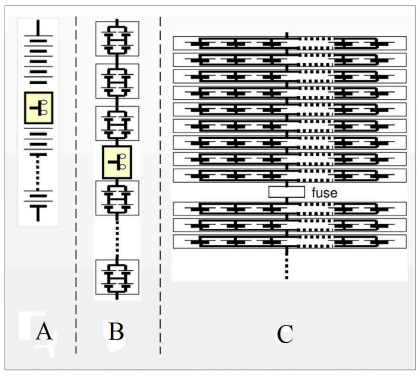

Fig. 1. Battery configurations A, B and C.

Whereas in topology (A), each cell constitutes a Single Point of Failure (SPoF). Topology (B) is called double strings topology where each two cells are connected in parallel together, which is called stage, and in serial with others. This kind of topology increases the reliability of the system when the voltage is only important and current drop is allowed. Because one of the cells for a parallel pair can fail without voltage dropping. However a cell failure results in half current. One cell fault affects performance only insignificantly in topology (C) because the voltage does not drop and the current will have small decrease. As is obvious, the battery pack (A) seems far more relevant for the broad marked in terms of prize and weight than the car pack (C). Thus it seems relevant to consider how the reliability of simpler configurations could be improved by inexpensive means adding only limited extra weight to the pack. Such means include the use of early anomaly detection to facilitate pre failure repair, voltage converters to allow cell faults at the expense of reduced current consumption as well as reconfiguration rails and extra cells in stand by.

3. ANOMALY DETECTION

We consider model based detection of anomalies in individual cells based on changes in characteristic model parameters. A suitable circuit model representing both Lead Acid and Lithium Ion Batteries is presented by the US National Renewable Energy Laboratory Bhangu et al. (2005) and shown in Fig. 2.

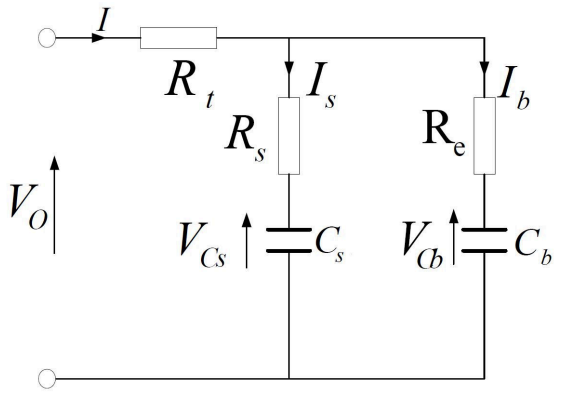

Fig. 2. General schematic of the RC battery model.

Where C_b is a bulk capacitor characterizing the ability of the battery to store charge, C_s is a capacitor modeling surface capacitance and diffusion effects within the cell, R_t is the terminal resistance, the surface resistance is showed by R_s, and R_e is end resistance. V_{Cb} and V_{Cs} are the voltage across the bulk and surface capacitors, and I is the current and from Kirchoff's laws, $I = I_b + I_s$.

To facilitate anomaly detection we transform the presented cirquit model in Bhangu et al. (2005) to a state space model

$$x = \begin{bmatrix} V_{Cb} \\ V_{Cs} \end{bmatrix} \tag{1}$$

$$\dot{x} = \begin{bmatrix} \frac{-1}{C_b(R_e+R_s)} & \frac{1}{C_b(R_e+R_s)} \\ \frac{1}{C_s(R_e+R_s)} & \frac{-1}{C_s(R_e+R_s)} \end{bmatrix} x + \begin{bmatrix} \frac{R_s}{C_b(R_e+R_s)} \\ \frac{R_e}{C_s(R_e+R_s)} \end{bmatrix} I$$

$$y = V_o = V_{Cb}\frac{R_e}{R_s+R_e} + V_{Cs}\frac{Rs}{R_s+R_e} + I\left(R_t + \frac{R_sR_e}{R_s+R_e}\right)$$

The obtained state space model differs from the one proposed in Bhangu et al. (2005), since we do not include the measured output voltage as a state, but rather as a measurement. Since the original network model shown in Fig. 2 comprises only two capacitors only a second order state space model is called for.
We estimate the values of the bulk capacity C_b and the terminal resistance since it is assumed that abnormal changes in these values may predict the future malfunction of the cell under consideration. Thus the state vector is augmented by C_b and R_t and their assumed fault dynamics. More precisely we estimate $\alpha = 1/C_b$ to avoid

numerical problems, i.e. division by zero. Parameter dynamics should be chosen to capture the timely evolution of parameters in case of faults. An immediate possibility is $d/dt\ \alpha = d/dt\ R_t = 0$ corresponding to Brownian parameter dynamics. Augmenting the state vector by α and R_t yields overall nonlinear dynamics

$$\begin{aligned} \dot{x} &= f(x,u) \\ y &= C(x,u) = V_o \end{aligned} \tag{2}$$

for which the relevant Jacobian is given by

$$f_x(x,u) = \begin{bmatrix} \frac{-1}{C_b(R_e+R_s)} & \frac{1}{C_b(R_e+R_s)} & \frac{V_{Cs}-V_{Cb}}{R_e+R_s} + I\frac{R_s}{Re+Rs} & 0 \\ \frac{1}{C_s(R_e+R_s)} & \frac{-1}{C_s(R_e+R_s)} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$C_x(x,u) = \begin{bmatrix} \frac{R_e}{R_s+R_e} & \frac{R_s}{R_s+R_e} & 0 & I \end{bmatrix}$$

State estimation is the general methodology applied for anomaly detection. anomaly is concluded when estimation error is systematically large. We apply an Extended Kalman Filter (EKF) for state estimation and use the estimated value of C_b to indicate anomaly. Alternatively the electrical states V_{Cb} and V_{Cs} may be considered. It seems however more convenient to compress detection into only one physical value that may be simply compared to its nominal value.

3.1 Active Detection

As given in equation (1) the current drawn from the cell acts as an input to the battery dynamics and output. Reliable detection of abnormal changes in the values of C_b and R_t therefore depends significantly on the current. Thus, periods without power consumption are not eligible for fault detection, which is of course of great practical inconvenience. We introduce an auxiliary current signal improving the detection of changes by optimizing the sensitivity of parameter changes to measurement signals. Indeed, since the EKF algorithm recursively solves a least squares estimation problem, we consider the squared error

$$E = \sum_{k=1}^{N}(y_k - \hat{y}_k)^2 = \sum_{k=1}^{N}(y_k(\theta^*) + e_k - y_k(\hat{\theta}))^2$$

where $\hat{\theta}$ contains the estimates of C_b and R_t and θ^* the true values, whereas $\{e_k\}$ is a white Gaussian sequence representing measurement noise. We approximate E close to the true parameter value θ^* by

$$E \approx \sum_{k=1}^{N}(\Delta_k(x,u)(\theta^* - \hat{\theta}) + e_k)^2$$

where

$$\Delta_k(x,u) = \frac{\partial y_k}{\partial \theta}|_{\theta^*,x,u}$$

Solving the LS optimization problem by $\frac{\partial E}{\partial \theta} = 0$ yields

$$\sum_{k=1}^{N}\Delta_k(x,u)\Delta_k^T(x,u)(\theta^* - \hat{\theta}) = \sum_{k=1}^{N}\Delta_k(x,u)e_k \tag{3}$$

It is readily seen that the estimate $\hat{\theta}$ is approximately unbiased. Thus, we select our auxiliary current signal to minimize the conditional number R of the matrix $\sum_{k=1}^{N}\Delta_k(x,u)\Delta_k^T(x,u)$ in order to reduce the variance of the estimate. This allows detection thresholds to be tighter and in turn facilitates reliable detection of smaller and earlier changes.

3.2 Design of auxiliary current signal

In the following, we assume the excitation input is a rectangular waveform as in Fig. 3. Its amplitude ϱ, time period T and duty cycle $\frac{\tau}{T}$ is designed such that the minimum R is obtained, i.e.

$$I = \varrho(\lceil\frac{t}{T}\rceil - \lceil\frac{t-\tau}{T}\rceil) \tag{4}$$

$$(\varrho, T, \tau) = \underset{\varrho,T,\tau}{\operatorname{argmin}}\ R \tag{5}$$

$$s.t. \begin{cases} P_{av} = V_o\ \varrho\ \frac{\tau}{T} \leq \bar{P} \\ 0 \leqslant \varrho \leqslant \varrho_{max} \\ 0 \leqslant \tau \leqslant \tau_{max} \\ T_{min} \leqslant T \leqslant T_{max} \end{cases}$$

where $\lceil\cdot\rceil$ denotes the ceil operation and P_{av} is the average

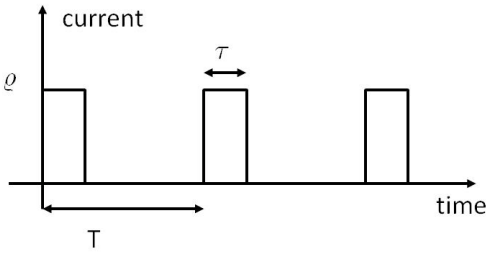

Fig. 3. Auxiliary discharge current

power consumption. The power constraint is natural in the sense that the detection algorithm should not comsume excess power. Similarly current limitations naturally bound the value of ϱ, whereas constraints on T and τ originate from computational feasibility considerations.

Equation (5) is non-convex and non-differentiable. To solve the problem with classical approaches, the problem must be changed to a convex problem by defining some constraints. Obtaining these constraints is not always feasible and is considered an open issue in the literature; see Mishra et al. (2009). Using evolutionary search algorithms such as GA, avoids having to change the problem to a convex one. As the optimization problem is calculated off-line, the computational effort is not important. The reader is referred to Chipperfield et al. (1994) for more details of the GA. Results from simulation are shown in Fig. 4, where the value of C_b is changed abruptly after 3500 seconds and that of R_t after 6500 seconds.

Overall both changes are tracked within 200-300 seconds although a certain bias and initial transient is present. The battery voltage has dropped only 0.01 volts over the entire detection period of 10000 seconds (3h), which seems

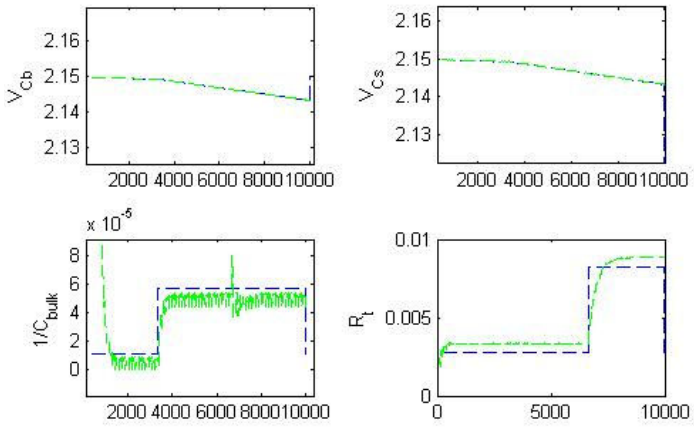

Fig. 4. Simulation results for abrupt changes of C_b and R_t.

reasonable compared to the discharge rates induced by normal operation.

4. RELIABILITY ASSESSMENT

The quantitative assessment of safety most often involves two major considerations; the frequency of failure and its consequence. Consequence is typically quantified as the number of casualties, severe injuries and lighter injuries, whereas frequency may be specified in terms of reliability profiles (lifetimes), probability of failure within the lifetime of a product or failure rates. Combining frequency and consequence an overall expected loss of life/health/assets may be found. Depending on its value it may be necessary to reduce either frequency or consequence to match the gained benefits of the product under consideration according to the as low as reasonably practicable (ALARP) principle, as in ALARP (2002). In this case we restrain to reliability considerations for safety assessment and disregard consequence/hazard analysis.

We especially use failure rates and the associated mean time to failure (MTTF) for quantitative comparison between configurations. Also we assume for all components to be located in the *useful lifetime* (UT) period of its overall life time. This means that early infant and end of life mortalities are disregarded. In the UT period the life time t_C of a battery cell may be modeled by an exponentially distributed random variable, i.e. $R_C(t) = P(t_C \geq t) = exp(-\lambda_C t)$, where λ_C is the fault rate of each cell and R_C is its reliability function.

From text book calculations the overall reliability function R_S of the single string of topology (A) is given by

$$R_S(t) = R_C^n(t) = exp(-n\lambda_C t) \tag{6}$$

where n is the number of cells in the string. The associated MTTF is given by

$$MTTF = \int_0^\infty R(t)dt \tag{7}$$

Taking $n = 88$ and $\lambda_C = 1E-6hour^{-1}$ we obtain $MTTF_C = (1/88)E6 = 1.1E4$ or around 15 months, which is from all perspectives a low number. The qualitative interpretation of particular MTTF values is assumed to follow the prevailing ISO 26262, standard in the area as in ISO26262 (2009), defining 4 Automotive Safety Integrity levels (ASIL); A (low safety critical) to ASIL D (high safety critical). Quantification to fault rates of ASIL levels A to D may be conducted by translation to the Safety Integrity Levels (SIL) 1-4 of the IEC 61508 standard, as in IEC61508 (1999). Such an interpretation is performed in Kandl (2010) and illustrated in Fig. 5, where PFH is probability of failure per hour.

PFH	SIL	ASIL
-	-	QM
$\geq 10^{-6}$ to $< 10^{-5}$	1	A
< 10.000		
$\geq 10^{-7}$ to $< 10^{-6}$	2	B
< 1.000		C
$\geq 10^{-8}$ to $< 10^{-7}$	3	
< 100		D
$\geq 10^{-9}$ to $< 10^{-8}$	4	-
< 10		

Fig. 5. ASIL/SIL relations from Kandl (2010).

As revealed by Fig. 5 the single string of topology (A) does not comply with even the lowest ASIL level. Taking instead the double parallel string of topology (B) and assuming that disconnection of malfunctioning cells is a hardwired feature, we obtain an MTTF for full current of $MTTF_D = (1/2/96)E6 = 5.2E3$ which is slightly lower than the previous one. Assuming however that half current is sufficient for safe operation, at the expense of comfort features like air-condition, another result emerges. Since each stage of two parallel cells is locally connected, one cell fault per stage may be sustained for half current operation. Thus we enumerate the reliability calculations according to the number j of single cell/stage faults and obtain

$$R_{D/2}(t) = \sum_{j=0}^{n} \binom{n}{j} 2^j (1 - R_C(t))^j R_C^{2n-j}(t) \tag{8}$$

and an associated MTTF

$$MTTF_{D/2} = \sum_{j=0}^{n} \sum_{k=0}^{j} \binom{n}{j} \binom{j}{k} 2^j (-1)^{j-k} \frac{1}{(2n-k)\lambda_C} \tag{9}$$

which for topology (B) (n=96) amounts to $MTTF_{D/2} = 0.98E5$ taking this configuration almost to the ASIL A level. Altogether one may conclude, that even advanced existing battery configurations only barely manage to fulfill even the most moderate standardized safety levels. Improving reliability properties may be achieved through hardware augmentation, e.g. additional battery cells in standby configuration and reconfiguration wires. Hardware augmentation is however undesirable for cost and weight reasons. The following section is devoted to the improvement and assessment of reliability properties of battery configurations through the application of early anomaly detection.

5. RELIABILITY IMPROVEMENT BY ANOMALY DETECTION

The impact of early detection on battery pack reliability relies on the possibility of pre failure repair. It is assumed that a detected anomaly is reported to the driver and urges him to visit a repair facility. Repair can be provoked by auxiliary means such as limiting the current drawn from

the battery and hereby limiting the acceleration and speed of the vehicle or by removing certain comfort services such as air condition or seat heating. A basic assumption leveraging the benefit of early detection is that repair can be provoked to be significantly faster than failure on the average.

5.1 Markovian modeling of detection-repair-fault process

Consider the single string of topology (A). We assume as above the lifetime t_C of each cell to be exponential and as such governed by a continuous time Markov process. The Markovian assumption is similarly adopted for the repair process as well as the lifetimes t_d and $t_C - t_d$, where t_d is the time until an anomaly is detected. Since $t_C = t_d + t_C - t_d$ there is a fundamental contradiction in assuming t_d, $t_C - t_d$ and t_C all being exponential. This is however neglected due to the approximative nature of the model. A graphical impression of the Markovian model is given in Fig. 6

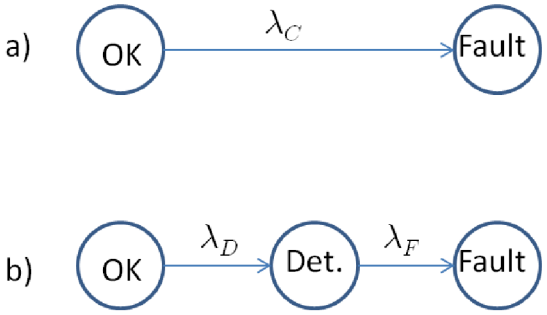

Fig. 6. Markov models with (b) and without (a) anomaly detection.

also indicating transition rates λ_C,λ_D and λ_F. To match expected cell lifetime in the model including anomaly detection we set $\lambda_C = 1/(1/\lambda_D + 1/\lambda_F)$. To parametrize the ability for early detection we let $\lambda_D = \alpha\lambda_F$ yielding $\lambda_F = (\alpha+1)/\alpha\ \lambda_C$. Similarly we parametrize the repair-to-fault speed ratio by $\lambda_R = \beta\lambda_C$.
An overall Markovian model is given in Fig. 7

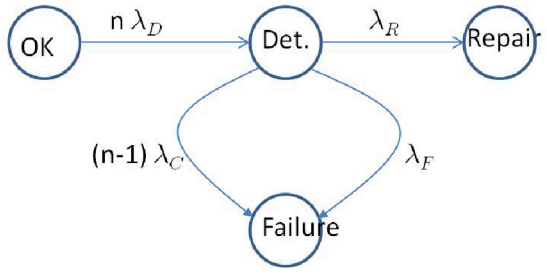

Fig. 7. Markovian model including detection, repair and entire battery pack.

We adopt a life-cycle approach for analysis, i.e. the battery, in its lifetime, passes through a number of repair cycles, where the first one starts when the new car is first driven and ends either in repair of the battery after an early warning or in battery failure in cases, where the driver did not have sufficient time to visit a repair facility. The probability P_R that repair is earlier than fault given by

$$P_R = \frac{\lambda_R}{(n-1)\lambda_C + \lambda_F + \lambda_R} = \frac{\beta}{(n-1) + \frac{\alpha+1}{\alpha} + \beta}$$

The conditional lifetime $t_{T|R}$ until transition out of the *Det.* (Detection) state, given repair is earlier than fault has a distribution

$$P(t_T \le t | t_R \le t_F) = 1 - exp(-((n-1)\lambda_C + \lambda_F + \lambda_R)t)$$

yielding a conditional mean time to repair $MTTR_R$ given by

$$MTTR_R = \frac{1}{(n-1)\lambda_C + \lambda_F + \lambda_R} + \frac{1}{n\lambda_D}$$
$$= \frac{1}{\lambda_C}\left(\frac{P_R}{\beta} + \frac{1}{n(\alpha+1)}\right)$$

The number of repair cycles until fault is geometrically distributed with a mean $1/(1-P_R)$. Thus we find the mean time to failure $MTTF$ by

$$MTTF = \frac{MTTR_R}{(1-P_R)} = \frac{1}{\lambda_C}\frac{\left(\frac{P_R}{\beta} + \frac{1}{n(\alpha+1)}\right)}{1-P_R}$$
$$= \frac{1}{\lambda_C}\left(\frac{1}{n-1+\frac{\alpha+1}{\alpha}} + \frac{n-1+\frac{\alpha+1}{\alpha}+\beta}{(n-1+\frac{\alpha+1}{\alpha})n(\alpha+1)}\right) \quad (10)$$

To obtain an operational overview we assume $\alpha < 1$, i.e. it is assumed that anomalies may only be detected in the late stages of the battery lifetime. We set as an example $\alpha = 0.1$. Also we assume $\beta >> 1$, i.e. the repair process is many times faster than the cell fault process. We even assume $\beta = Bn$ for $B > 1$ indicating that the repair process is even faster than the compound fault process of all cells in the pack. As an example we set $B = 10$, which for $\lambda_C = 1E-6$ and $n \approx 100$ yields $\lambda_R = 1E-3$ or a mean time to repair of approximately 42 days, which seems reasonable. In this case we get

$$MTTF \approx \frac{12}{n\lambda_C} \quad (11)$$

or approximately 12 times as high as for the case without early detection, which takes this configuration to the ASIL A level.

Similarly we may investigate how reliability is improved by early detection in the double parallel string of the battery pack (B). The Markov model in Fig. 7 needs to be modified as shown in Fig. 8.

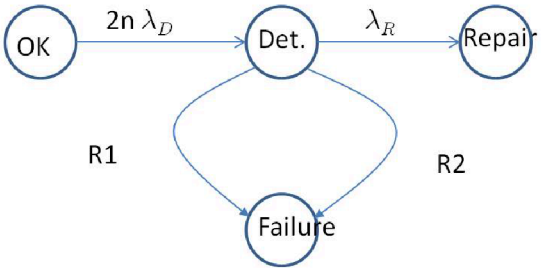

Fig. 8. Modified abstract Markovian model for the the battery pack (B), double parallel string with early detection.

In Fig. 8 the parallel lifetimes governing transition from state *Det.* to state *Failure* are no longer exponential. They are however generated by an underlying Markov model with exponential transitions. Thus we refer to the model in Fig. 8 as an *abstract Markov model*. After the first

detected anomaly, we conceptually isolate the stage, where the anomaly is detected. This stage causes failure if the abnormal cell fails along with its parallel peer.
Remaining cells exhibits a lifetime depending on whether a full or half current requirement is adopted. For full current the lifetime R_1 of remaining cells is exponential with rate $2(n-1)\lambda_C$, while for half current $R_1 = R_{D/2}$ as given in (8) and for $n \to n-1$, i.e. number of stages decremented by one to omit the abnormal stage.
The overall reliability R for the transition from state *Det* to *Failure* is given by $R = R_1 \cdot R_2$, since fault processes of the abnormal stage and the remaining pack are considered independent.
Again we consider the conditional lifetime R_{Rc} of the time to enter state *Repair*, given by

$$R_{Rc}(t) = \frac{\int_t^\infty f_R(\varsigma)R(\varsigma)d\varsigma}{P_R} \tag{12}$$

where f_R is the density function given by $f_R = -d/dtR_R$, R_R is the unconditional repair lifetime and P_R is the probability of reaching the *Repair* state before failure, i.e.

$$P_R = \int_0^\infty f_R(\varsigma)R(\varsigma)d\varsigma \tag{13}$$

The conditional $MTTR_R$ is then found by

$$MTTR_R = \int_0^\infty R_{Rc}(\varsigma)d\varsigma \tag{14}$$

Expecting on the average $1/(1-P_R)$ successful repair cycles, we obtain $MTTF_D = 9.4E3$ and $MTTF_{D/2} = 1.04E5$, which for the full current result is considered a significant improvement but for half current rather insignificant. The latter is explained by the high level of redundancy exhibited when half current is allowed.

6. CONCLUSION

This paper presents a novel active fault detection methodology for early prediction of potential cell failures in a variety of high-voltage battery topologies for electric vehicles. First, reliability and MTTF of reference single and double string topologies are calculated. It is shown that without fault detection and fault control algorithm, such topologies cannot fulfill standardized safety levels. The proposed early anomaly detection algorithm draws auxiliary current from battery, which improves the failure detection by optimizing the sensitivity of parameter changes to measurement signals. It is shown that combining this algorithm with a pre-failure warning signal that instructs the driver to visit a repair facility improves MTTF significantly. Future work will focus on evaluating the proposed methodology via simulations and experimental studies. Furthermore, we will investigate whether this methodology is generally applicable by applying it to different electric vehicle systems, such as steering.

REFERENCES

Affanni, A., Bellini, A., Franceschini, G., Guglielmi, P., and Tassoni, C. (2005). Battery choice and management for new-generation electric vehicles. *Industrial Electronics, IEEE Transactions on*, 52(5), 1343–1349.

ALARP (2002). Cost benefit analysis (cba) checklist. *Journal of Process Control*. URL `http://www.hse.gov.uk/risk/theory/alarpcheck.htm`.

Anwar, S. (2010). Fault detection, isolation, and control of drive by wire systems. *InTech*, 24.

Bhangu, B., Bentley, P., Stone, D., and Bingham, C. (2005). Nonlinear observers for predicting state-of-charge and state-of-health of lead-acid batteries for hybrid-electric vehicles. *Vehicular Technology, IEEE Transactions on*, 54(3), 783–794.

Chatzakis, J., Kalaitzakis, K., Voulgaris, N., and Manias, S. (2003). Designing a new generalized battery management system. *Industrial Electronics, IEEE Transactions on*, 50(5), 990–999.

Chipperfield, A., Fleming, P., Pohlheim, H., and Fonseca, C. (1994). Genetic Algorithm Toolbox for use with MATLAB.

Gholami, M., Schiler, H., and Bak, T. (2011a). Active fault diagnosis for hybrid systems based on sensitivity analysis and adaptive filter. In *Accepted in IEEE Multi-Conference on Systems and Control * September 28-30, 2011 * Denver, CO 80202, USA*.

Gholami, M., Schiler, H., and Bak, T. (2011b). Active fault diagnosis for hybrid systems based on sensitivity analysis and ekf. In *American Control Conference (ACC 2011), accepted*.

Hagen, R., Chen, K., Comte, C., Knudson, O., and Rouillard, J. (2000). Fault-tolerant battery system employing intra-battery network architecture. US Patent 6,104,967.

IEC61508 (1999). International electrotechnical commission. iec 61508:functional safety of electrical/ electronic/ programmable safety-related systems, 1999.

ISO26262 (2009). International organization for standardization. iso 26262:road vehicles - functional safety, 2009.

Kandl, S. (2010). *A Requirement-Based Systematic Test-Case Generation Method for Safety-Critical Embedded Systems*. Ph.D. thesis, Technischen Universitat Wien.

Laidig, M.R. and Wurst, J.W. (2006). Battery failure prediction. Technical report, BTECH, Inc.

Mishra, S., Wang, S., and Lai, K. (2009). *Generalized convexity and vector optimization*. Springer Verlag.

Stuart, T., Ashtiani, C., Pesaran, A., Fang, F., and Wang, X. (2002). A modular battery management system for hevs. In *Proceedings of the SAE Future Car Congress (Paper Number 2002-01-1918), Arlington, VA*.

Weng, S. (2009). Intelligent fault-tolerant battery management system. US Patent App. 20,090/206,841.