Energy Management System for Automated Driving

Optimal and Adaptive Control Strategy for Normal and Failure Case Operation

Kirill Gorelik, Ahmet Kilic
Corporate Sector Research and Advance Engineering
Robert Bosch GmbH
Renningen, 71272, Germany
Email: {kirill.gorelik, ahmet.kilic}@de.bosch.com

Roman Obermaisser
Institute of Embedded Systems
University of Siegen
Siegen, 57068, Germany
Email: roman.obermaisser@uni-siegen.de

***Abstract*—With increasing level of driving automation new requirements regarding reliable power supply for power net components arise. In addition to new fail-operational power nets, appropriate control strategies providing functional power supply at least for the duration of vehicle transition to a safe state (standstill) are required. This paper presents a generic, topology-independent concept for future energy management systems controlling fail-operational power nets for automated driving in both normal and failure cases. Based on predictive runtime energy flow optimization and a 3-level-degradation concept, the energy management system presented in this work allocates the available power net energy resources in a way allowing to bring the vehicle to a standstill at the safest location with the best-suited driving profile and with the maximum of driving comfort. By adapting the control strategy to the current system state, the energy management system enables reliable power supply for power net components and increases the overall energy efficiency.**

Keywords—Energy Management System, Automated Driving, Functional Safety Concept, Fail-Operational Power Nets

I. Introduction

With increasing numbers of driver assistance systems in road vehicles, partly or fully taking over the control over longitudinal and/or literal vehicle guidance, new requirements regarding safety and reliability for the electrical power supply of safety-critical components arise. Upcoming new driving automation technologies continuously relieve the driver from his role as fallback in case of a system or component failure. Starting with highly and fully automated driving (SAE automation level 4 and 5), the system must cope with all driving tasks without driver interaction and supervision in specified use cases for high automation and in all use cases for full automation [1]. Therefore, a fail-operational power net guaranteeing functional power supply of safety-critical components like sensors, actuators and vehicle guidance logic at least for the duration of transitioning to a safe state (vehicle standstill) is required [2, 3].

The increasing complexity of fail-operational power net topologies for automated driving implicates new degrees of freedom for control strategies due to the increasing number of components used for power distribution and energy storage. New strategies for optimal control of fail-operational power nets are required, enabling reliable power supply for safety-critical components and adaptability to possible failures occurring during automated driving. The work presented in this paper describes a new concept for energy management systems (EMS) controlling fail-operational power nets for automated driving.

II. State of the Art in Energy Management Systems

The main task of a supervisory control algorithm for a complex system is to find and set an optimal operating point for achieving the goals defined for this system [4]. Control strategies can be divided into heuristic and optimal. Heuristic control strategies are based on predefined, intuitive rules, while optimal control strategies are based on a theory of optimal control, requiring a mathematical model of the system and a definition of the cost function reflecting the goals to be achieved by the system depending on system variables [5]. The optimal operating point can be found by minimizing or maximizing the cost function under system constraints either during the runtime (online) or for performance benchmarks of a heuristic control strategy (offline) [5]. A control strategy is causal if it is based only on knowledge about present and past system behavior, and non-causal if also the knowledge about future system behavior is required [5]. By using predicted future system behavior, online optimal control strategies can be implemented [5].

An energy management system can be defined as a supervisory control algorithm for a vehicle power net with the primary goal of energy-efficient power distribution. A lot of research was investigated into energy management systems for vehicles with internal combustion engine (ICE) only [6], hybrid electric vehicles (HEV) [7, 8, 9, 10, 11, 12] and fully electric vehicles (EV) [13]. The main goals of these control strategies are higher energy efficiency for ICE-based vehicles and HEVs [6, 7, 8, 9, 10, 11, 12], range extensions for EVs [13], improvement of driving dynamics and comfort [6, 7, 9, 11, 12, 13], stress reduction for power net components [7] and reduction of driving time [9]. All these control strategies have in common that they are designed for a non fail-operational, specific system configuration (i.e., topology-dependent control strategy), considering only the case of normal operation. Therefore, the algorithm for the control strategy must be adapted if the system configuration is changed. In addition, reliable power supply of safety-critical components in case of a failure is also not covered. Since safety-critical components are

978-1-5090-4623-2/17/$31.00 ©2017 IEEE

required for the transition to a safe state (standstill), these control strategies are not suitable for highly and fully automated driving.

III. Motivation and Goals

As shown in Section I and II, one of the main requirements for fail-operational power nets used for automated driving is to guarantee reliable power supply for safety-critical functions for the duration of transitioning to a safe state in case of a system failure. In accordance to ISO 26262:2011, establishing reliable power supply for safety-critical functions becomes a functional safety requirement [14]. For fulfilling this requirement, new fault-tolerant power net topologies are required on the one hand [2, 3]. On the other hand, a functional safety concept is required for the EMS controlling a fault-tolerant power net.

One approach for developing a functional safety concept for an EMS could be identifying and analyzing all possible power net failure states and defining a reaction for each single failure. This approach would lead to a rule- and topology-based control strategy and safety concept, requiring time consuming failure analysis, definition and verification of failure reactions for each power net configuration and topology, with no guarantee that the assumed fault hypothesis is complete.

As mentioned in Section I and II, a safe state that must be reached in case of a system failure for a vehicle with automated driving is standstill. However, the scenario of transitioning to the standstill may be different, starting with driving to the destination set by the user/passenger and parking the vehicle at that destination as the best case scenario and ending with emergency braking and stopping the vehicle at the same driving lane as the worst case scenario (for details see Section VI). A rule-based functional safety concept would also mean, that for each single possible failure a fixed scenario for transitioning to a safe state must be defined, making the verification that the safe state will be reached under all conditions even more time consuming and topology-dependent. Slight changes in the power net topology and/or dimensioning of power net components would require a new iteration of verification. Additionally, considering the point that the verification of the safety concept is done under certain assumptions and modeling limitations for components of the power net as well as for vehicle environment conditions, it becomes clear that the safety concept could be weakened by the uncertainty in the assumptions made.

As mentioned in Section II, one of the main goals in the state of the art of EMS is to increase the energy efficiency of the system. This goal is achieved by optimizing and reducing the system energy consumption. The aspect of energy distribution is not considered due to the lack of configurability at the system level. Considering the power net topologies used for automated driving, redundancies might be needed to fulfil the requirement for the fail-operational power supply. Building redundancies means using additional power net components, thus leading to a higher degree of freedom on system level as needed for optimization of power distribution.

The first main goal for the EMS proposed in this paper is a generic control strategy of a distributed fail-operational power net for automated driving which is independent from its topology and component's dimensioning. It is assumed that a vehicle power net consists of up to n ($n \geq 1$) sub power nets connected to each other via power links. The concept for the generic EMS presented in this paper could be used in a vehicle with a combustion engine only as well as in hybrid and pure electric vehicles. The examples presented in this paper will focus on power net topologies for pure electric vehicles without limitation of generality. The adoption of the generic EMS to a specific vehicle type does not require any changes in the control algorithm and functional safety concept and is done by configuring and parametrizing the EMS only. For achieving this goal, an architecture for the EMS will be proposed in Section IV and a mathematical description and abstraction of distributed, fail-operational power nets in Section V.

The second main goal for the EMS is to optimize the energy distribution in a way that the remaining energy resources available in the vehicle will be maximized both for normal operation and failure cases. Runtime diagnostic information and current states of power net components will be taken into account for energy flow optimization. The definition of the optimization problem and the system constrains necessary for achieving this goal is presented in Section V.

The third and also the most important goal from the perspective of functional safety is to control the power net in a way that the vehicle comes to the standstill at the safest possible location. An additional non-functional requirement for the EMS is to provide the maximum possible driving comfort and best suited driving profile for normal operation as well as for failure cases. For achieving these requirements, a 3-level-degradation concept, based on predicted data for the driving profile, available energy resources and energy demand for propulsion as well as for safety critical and comfort functions was developed and is presented in Section VI. The three levels of the degradation concept are in particular degradation of the load profile for comfort functions, degradation of the driving profile (velocity and acceleration) and degradation of the destination that must be reached for the standstill.

Summing up the goals and requirements, the EMS presented in this work is an adaptive and online optimized, topology-independent control strategy with the main goal of reliable and energy-efficient power supply and energy distribution for fail-operational power net topologies used for automated driving, covering both the normal and failure case operation.

IV. Architecture of the Energy Management System

For achieving the goals defined in Section III, a functional architecture for EMS as shown in Fig. 1 is proposed. It is assumed that a vehicle power net consists of up to n ($n \geq 1$) sub power nets. Each sub power net k is controlled and monitored by a related sub energy management system k (Sub EMS k) with $k \in \{1..n\}$. The generic control algorithm for Sub EMS is adapted to a given sub power net topology via a configuration file (config k), containing all relevant information about the components of this sub power net. This information includes for example the number of energy storages (which could also be zero) and their nominal capacities, energy consumption of safety related and comfort components including their

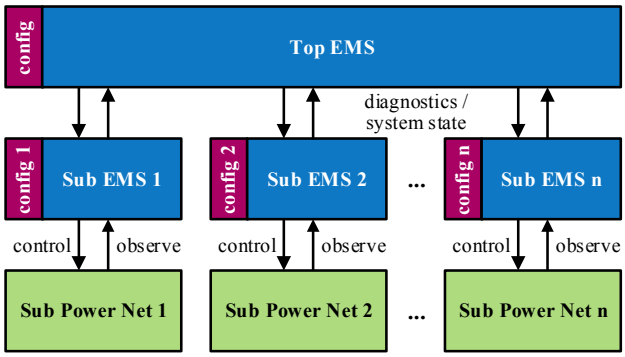

Fig. 1. Functional architecture of energy management system.

degradation profiles. The Sub EMS observes during runtime the current state of components related to the sub power net and receives diagnostic information, making it possible to initiate local reactions to abnormalities or component failures without involvement of the top-level energy management system (Top EMS), which is responsible for control and failure reactions at system level (vehicle power net consisting of n sub power nets).

The main task of the Top EMS is to ensure reliable power supply of safety related components by optimizing the energy flow at system level and to allocate sufficient energy resources to each sub power net for completing a driving cycle. The generic Top EMS is adapted to a given system topology via a configuration file, containing all relevant system information. This includes for example the number of sub power nets, efficiency maps for propulsion components and for power links connecting the sub power nets, vehicle parameters needed for predicting the amount of energy required for propulsion etc. Based on this data and runtime information received from Sub EMS, the Top EMS is able to optimize the energy flow, to adapt the control strategy to the current system state and to initiate reactions to abnormalities or failures at system level.

V. Energy Flow Optimization

For achieving the goals of the EMS as defined in Section III, an implementation of predictive and adaptive runtime energy flow optimization is proposed. In Section V-A, a mathematical model describing and abstracting distributed power nets consisting of up to n ($n \geq 1$) sub power nets will be presented. Based on this mathematical model, the cost function and the system constraints for the optimization problem will be defined in Section V-B. For adapting the energy flow optimization of the EMS to the current state of the power net, its components and runtime diagnostic information, an algorithmic structure representing the system state is needed. An appropriate matrix-based power net description will be presented in Section V-C. The mathematical formulation of the optimization problem will be presented in Section V-D.

A. Mathematical Power Net Model

For simplifying the notation, the following convention is used for the energy analysis of a power net consisting of up to n ($n \geq 1$) sub power nets. Index k ($k \in \{1..n\}$) identifies the sub power net for which the current energy analysis is considered. As illustrated in Fig. 2 and 3, the sub power net k could be connected to a set of other sub power nets (up to n-1) identified by index i ($i \in \{1..n\}\backslash\{k\}$) via power links $PL_{i,k}$ at its inputs $P_{in\_i,k}$ and $PL_{k,i}$ at its outputs $P_{out\_k,i}$. A power link connecting two sub power nets could be a DC/DC converter, a switch, a toggle switch or any other component enabling energy flow. The power link $PL_{i,k}$ transports the energy from the sub power net i to k and $PL_{k,i}$ from k to i. $E_{out\_i,k}$ denotes the amount of energy flowing from the sub power net i to k with the efficiency $\eta_{i,k}$ and the following equation could be used for describing the energy available at the input $P_{in\_i,k}$:

$$E_{in\_i,k} = \eta_{i,k} E_{out\_i,k} \tag{1}$$

The energy flow from sub power net i to k and from k to i is only possible, if both sub power nets are operational. A sub power net is considered to be operational if it has at least one functional energy storage or at least one functional connection to any other functional sub power net. The set of all operational sub power nets is denoted by "OPR" (OPeRational).

Furthermore, it is assumed that all components of a sub power net k could be classified and grouped into four classes. As illustrated in Fig. 2 and 3, the four component classes are in particular the energy storage components B_k with the total available energy E_{bat_k}, the safety related components R_{s_k} with the total energy demand E_{rs_k}, the comfort components R_{c_k} and the propulsion components R_{pr_k} with the total energy demand E_{rc_k} and E_{pr_k}. Under these assumptions and by defining the total energy demand E_{load_k} as

$$E_{load\_k} = E_{rs\_k} + E_{rc\_k} + E_{pr\_k}, \tag{2}$$

the following equation can be used for describing the energy balance E_{spn_k} of the sub power net k:

$$E_{spn\_k} = \sum_{\substack{i=1,i\neq k \\ i,k\in OPR}}^{n} (E_{in\_i,k} - E_{out\_k,i}) + E_{bat\_k} - E_{load\_k} \tag{3}$$

So the energy balance of a sub power net k can be expressed as a function of the predicted energy resources (E_{bat_k}), energy demands (E_{load_k}) and all energy flows at its inputs and outputs.

B. Definition of Cost Function and Constraints

Using predicted values for the energy resources E_{bat_k} and the total energy demand E_{load_k}, a sub power net k can be classified as a "sink" or as a "source". If the energy resources of a sub power net k are smaller than the total energy demand, then the sub power net k can be classified as a sink. If the energy resources are greater than the total energy demand, then the sub power net k can be classified as a source. The set "SRC" (SouRCe) of all sub power nets classified as a source is defined as:

$$SRC = \{\, k \,|\, (E_{bat\_k} - E_{load\_k} > 0) \wedge (k \in 1..n) \,\} \tag{4}$$

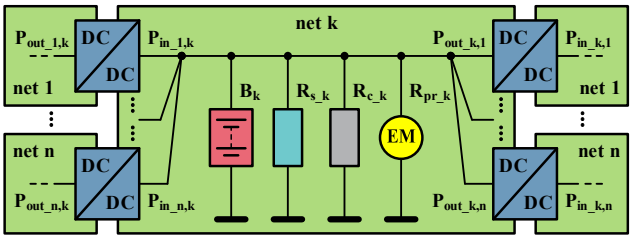

Fig. 2. Electrical block diagram of sub power net k.

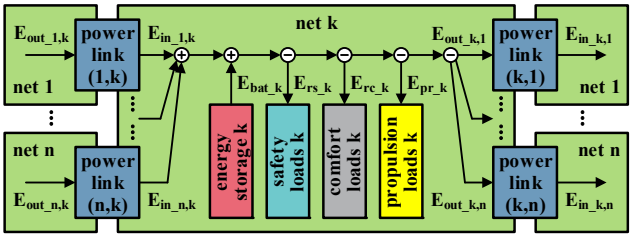

Fig. 3. Energy flow diagram of sub power net k.

As mentioned in Section III, one of the goals of the EMS presented in this work is to increase the energy efficiency of the power net by optimizing the energy flow. For achieving this goal, the approach proposed in this work is to maximize the amount of the energy resources available in the power net after completing a driving cycle. Since the EMS should cover both normal and failure cases, a driving cycle is considered to be completed after transitioning the vehicle to a standstill at the location selected by the control algorithm, which is not necessarily the destination set by the user/passenger.

Maximizing the amount of the energy resources available in the power net after completing a driving cycle would mean to maximize the sum of the energy balance values E_{spn_k} of all functional sub power nets considered to be a source. So the cost function used for the energy flow optimization can be defined as:

$$J(E_{out}) = \sum_{i \in SRC \cap OPR}^{n} E_{spn\_i} \tag{5}$$

By using (1) and (3), (5) can be rewritten as:

$$J(E_{out}) = \sum_{i \in SRC \cap OPR}^{n} \sum_{j \in OPR, j \neq i}^{n} \left(\eta_{j,i} E_{out\_j,i} - E_{out\_i,j}\right) + \sum_{i \in SRC \cap OPR}^{n} \left(E_{bat\_i} - E_{load\_i}\right) \tag{6}$$

For guaranteeing reliable power supply for the duration of a driving cycle, the energy resources in each sub power net k must be greater or equal to the total energy demand in this sub power net. This implies as a constraint for the energy flow optimization with the cost function as defined in (6), that the energy balance E_{spn_k} must be greater or equal to zero for all sub power nets. If one sub power net is not operational and it is not possible to achieve the energy balance in this sub power net, the EMS will optimize the energy flow by establishing the energy balance in the remaining functional sub power nets only. So the following constraint for the energy flow optimization can be defined:

$$E_{spn\_k} \geq 0 \quad \forall (k \in 1..n) \wedge (k \in OPR) \tag{7}$$

As illustrated in Fig. 2 and 3, the energy flow from the sub power net i to k is denoted by $E_{out\_i,k}$ and from k to i by $E_{out\_k,i}$. Using this notation, all energy flows from one sub power net to another one are greater or equal zero. This implies the last constraint for the energy flow optimization:

$$E_{out\_i,k} \geq 0 \quad \forall (i,k \in 1..n) \wedge (i \neq k) \tag{8}$$

Summing up the results, the energy flow optimization with the main goal of increasing the energy efficiency and guaranteeing a reliable power supply is based on the cost function as defined in (6). By maximizing the cost function under system constraints as defined in (7) and (8), the energy resources stored in a power net by completing a driving cycle are maximized, thus reducing the energy losses in components used for the power distribution to a minimum and providing sufficient energy resources allocated to all functional sub power nets for completing the driving cycle.

C. *Matrix Representation of System States and Variables*

For solving the optimization problem for the energy flow at runtime, an appropriate, computer-based representation of the system states and variables of a power net is required. A vector- and matrix-based representation, which can be easily implemented as a one- and two-dimensional array, is used for the optimization algorithm of the EMS presented in this work.

As described in Section V-A, a sub power net k could have up to n-1 outputs $E_{out\_k,i}$ ($i \in \{1..n\} \backslash \{k\}$). Thus, the total number of outputs of a power net consisting of n sub power nets equals (n-1)*n. All these outputs can be represented by an n-by-n output matrix $\underline{E}_{out}$ as shown in (9):

$$\underline{E}_{out}^{n \times n}(t) = \begin{pmatrix} E_{out\_1,1}(t) & \cdots & E_{out\_1,n}(t) \\ \vdots & \ddots & \vdots \\ E_{out\_n,1}(t) & \cdots & E_{out\_n,n}(t) \end{pmatrix} \tag{9}$$

Matrix element $E_{out\_i,j}$ describes the energy flow from sub power net i to j. Energy flow in the reverse direction (from j to i) is represented by the element $E_{out\_j,i}$. The time-dependency of the matrix elements indicates that the output energy is allocated at runtime as a function of current system states and diagnostic information. Since the elements $E_{out\_i,i}$ ($i \in \{1..n\}$) have no physical meaning, they are set to zero.

In a similar way, the efficiency matrix can be defined. As shown in (10), the n-by-n efficiency matrix $\underline{\eta}$ describes the current energy flow efficiencies of the (n-1)*n power links connecting n sub power nets with n-1 outputs each:

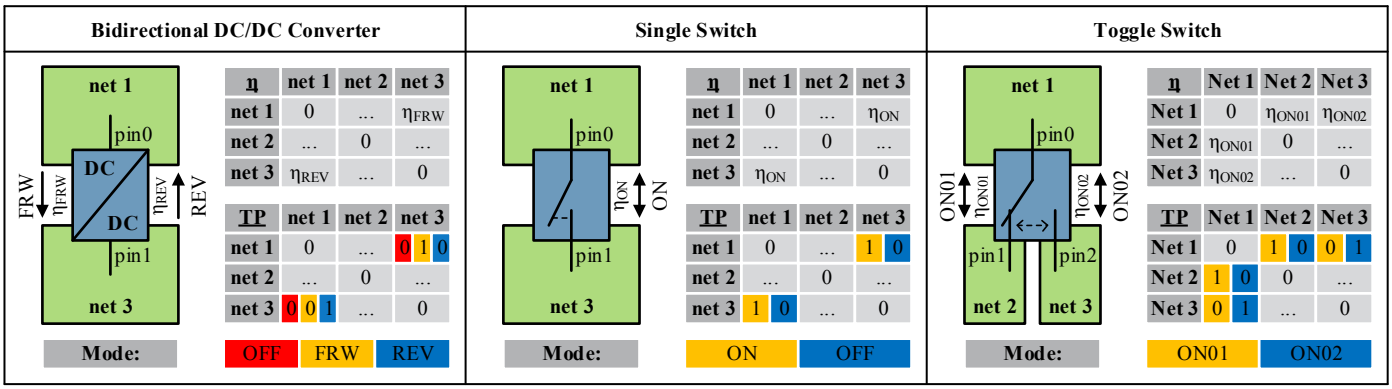

Fig. 4. Representation of a bidirectional DC/DC converter (left), a single switch (middle) and a toggle switch (right) with efficiency and topology matrices.

$$\underline{\eta}^{n\times n}(t)=\begin{pmatrix}\eta_{1,1}(t)\cdots\eta_{1,n}(t)\\ \vdots\quad\ddots\quad\vdots\\ \eta_{n,1}(t)\cdots\eta_{n,n}(t)\end{pmatrix} \tag{10}$$

The time-dependency of the matrix elements indicates again the real-time behavior of the energy management algorithm. So, for example, a failure in a power link, resulting in a decrease of the energy flow efficiency, will be considered at runtime by the energy flow optimization algorithm.

The energy flow efficiency matrix alone is not sufficient for implementing the optimization algorithm. Also the description of all valid and active power links and their configurations is needed. The topology matrix $\underline{TP}$ as defined in (11) is used for describing the status of up to n*(n-1) possible power link connections:

$$\underline{TP}^{n\times n}(t)=\begin{pmatrix}TP_{1,1}(t)\cdots TP_{1,n}(t)\\ \vdots\quad\ddots\quad\vdots\\ TP_{n,1}(t)\cdots TP_{n,n}(t)\end{pmatrix} \tag{11}$$

If the energy flow from sub power net i to j is activated and functional, then the value of the matrix element $TP_{i,j}$ is set to 1, else to 0. The status of the energy flow in the reverse direction (from j to i) is represented by the matrix element $TP_{j,i}$. Since the elements $\eta_{i,i}$ and $TP_{i,i}$ ($i \in \{1..n\}$) of the efficiency and topology matrix have no physical meaning they are set to zero.

The use of the efficiency and topology matrices for the description of typical components enabling energy flow will be exemplified subsequently for a bidirectional DC/DC converter, a single and a toggle switch. As illustrated in Fig. 4, it is assumed that a bidirectional DC/DC converter connecting the sub power nets 1 and 3 can be operated in three modes. In forward mode, the energy flows from net 1 to 3 with the efficiency η_{FWD}, so the element $\eta_{1,3}$ of the efficiency matrix is set to this value. In the reverse mode, the energy flows from net 3 to 1 with the efficiency η_{REV}, stored in the matrix element $\eta_{3,1}$. If the DC/DC converter is deactivated (OFF), both elements $TP_{1,3}$ and $TP_{3,1}$ of the topology matrix are set to 0. Functional active forward mode (FRW) is represented by setting $TP_{1,3}$ to 1 and $TP_{3,1}$ to 0, the reverse mode (REV) by setting $TP_{1,3}$ to 0 and $TP_{3,1}$ to 1. A failure in a connection, e.g. open connection, is simply represented by setting the associated topology matrix element to 0. An activated single switch connecting the nets 1 and 3 as illustrated in Fig. 4 allows the energy flow in both, forward and reverse direction. By denoting the efficiency of the switch by η_{ON}, the elements $\eta_{1,3}$ and $\eta_{3,1}$ of the efficiency matrix must be set to this value. The elements $TP_{1,3}$ and $TP_{3,1}$ of the topology matrix are set to 1 for an active switch connection (ON), and to 0 for a deactivated switch connection (OFF).

In a similar way, a toggle switch connecting the nets 1, 2 and 3 can be represented as illustrated in Fig. 4. Denoting the efficiency of the energy flow between net 1 and 2 by η_{ON01}, and between 1 and 3 by η_{ON02}, the matrix elements $\eta_{1,2}$ and $\eta_{2,1}$ are set to η_{ON01}, and $\eta_{1,3}$ and $\eta_{3,1}$ to η_{ON02}. The active functional connection between pin0 and pin1 (ON01) implies the elements $TP_{1,2}$ and $TP_{2,1}$ to be set to 1 and the elements $TP_{1,3}$ and $TP_{3,1}$ to be "toggled" to 0. The active functional connection between pin0 and pin2 (ON02) implies inverse values for the elements $TP_{1,2}$ / $TP_{2,1}$ (set to 0) and for $TP_{1,3}$ / $TP_{3,1}$ (set to 1).

The predicted energy resources $\underline{E}_{bat\_i}$ and total energy demands $\underline{E}_{load\_i}$ ($k \in \{1..k\}$) of k sub power nets are represented by the vectors $\underline{E}_{bat}$ and $\underline{E}_{load}$ as shown in (12):

$$\underline{E}_{bat}^{n\times 1}(t)=\begin{pmatrix}E_{bat\_1}(t)\\ \vdots\\ E_{bat\_n}(t)\end{pmatrix},\quad \underline{E}_{load}^{n\times 1}(t)=\begin{pmatrix}E_{load\_1}(t)\\ \vdots\\ E_{load\_n}(t)\end{pmatrix} \tag{12}$$

The vector elements $\underline{E}_{bat\_i}$ and $\underline{E}_{load\_i}$ ($i \in \{1..n\}$) store the predicted values for the sub power net i. The time dependency of the vector elements indicates again the real-time aspect of the EMS, which adapts its control strategy to any detected changes and failures at system and component levels, e.g. a change in the battery capacity or increase of the average energy consumption of a load due to a failure.

For the description of the sub power net state, two vectors $\underline{ST}_{opr}$ and $\underline{ST}_{src}$ as defined in (13) are used:

$$\underline{ST}_{opr}^{n\times 1}(t)=\begin{pmatrix}ST_{opr\_1}(t)\\ \vdots\\ ST_{opr\_n}(t)\end{pmatrix},\quad \underline{ST}_{src}^{n\times 1}(t)=\begin{pmatrix}ST_{src\_1}(t)\\ \vdots\\ ST_{src\_n}(t)\end{pmatrix} \tag{13}$$

If a sub power net i belongs to the set OPR of sub power nets classified as operational, then the element ST_{opr_i} of the state vector $\underline{ST}_{opr}$ is set to 1, else to 0. The definition of the source state vector $\underline{ST}_{src}$ is similar. If a sub power net i belongs to the set SRC of sub power nets classified as a source, then the vector element ST_{src_i} is set to 1, else to 0.

D. *Formulation of the Energy Flow Optimization Problem*

For the formulation of the energy flow optimization problem based on matrix and vector system representation as defined in Section V-C, an elementwise matrix multiplication as shown in (14) and denoted by a white bullet '∘' is needed:

$$\underline{A}^{n\times n} \circ \underline{B}^{n\times n} = (a_{ij}) \circ (b_{ij}) = (a_{ij} b_{ij}) \quad \forall (i, j \in 1..n) \tag{14}$$

A normal matrix multiplication is denoted by a black bullet '·'. Using these definitions, the energy balance $\underline{E}_{spn}$ of all n sub power nets as defined in (3) can be rewritten as:

$$\begin{aligned} \underline{E}_{spn}^{n\times 1} = {} & \underline{ST}_{opr}^{n\times 1} \circ [(\underline{\eta}^{n\times n} \circ \underline{TP}^{n\times n} \circ \underline{E}_{out}^{n\times n})^{T} \cdot \underline{ST}_{opr}^{n\times 1}] \\ & - \underline{ST}_{opr}^{n\times 1} \circ [(\underline{TP}^{n\times n} \circ \underline{E}_{out}^{n\times n}) \cdot \underline{ST}_{opr}^{n\times 1}] \\ & + \underline{ST}_{opr}^{n\times 1} \circ [\underline{E}_{bat}^{n\times 1} - \underline{E}_{load}^{n\times 1}] \end{aligned} \tag{15}$$

The cost function as defined in (6) can be rewritten as:

$$J(\underline{E}_{out}^{n\times n}) = (\underline{ST}_{src}^{n\times 1})^{T} \cdot \underline{E}_{spn}^{n\times 1}(\underline{E}_{out}^{n\times n}) \tag{16}$$

So the energy flow optimization problem can be defined as:

$$\begin{aligned} \max \quad & J(\underline{E}_{out}^{n\times n}) = (\underline{ST}_{src}^{n\times 1})^{T} \cdot \underline{E}_{spn}^{n\times 1}(\underline{E}_{out}^{n\times n}) \\ \text{s.t.} \quad & [\underline{E}_{spn}^{n\times 1}(\underline{E}_{out}^{n\times n}) \geq 0] \wedge [\underline{E}_{out}^{n\times n} \geq 0] \end{aligned} \tag{17}$$

Adaptive energy flow optimization presented in this work minimizes the energy losses in components used for energy distribution and allocates the available energy resources to all functional sub power nets in a way allowing to complete a driving cycle. The variables used for the optimization are the output energies of the sub power nets, which are changed by using different operating modes for the power link components. If no valid solution is found, meaning the overall energy resources are smaller than the total energy demand of the system, a degradation concept for reduction of the overall system energy demand is needed. A 3-level-degradation concept used in this work will be presented in Section VI.

VI. Degradation Concept

Driving to the safest possible location with the best-suited driving profile and with the maximum of driving comfort at the current power net state is one of the goals defined for the EMS in Section III. Section VI-A gives an overview of the possible safe state locations and their prioritization used by the EMS. A degradation concept used for achieving the defined goals will be presented in Section VI-B.

symbol	destination	prio	name	energy demand
	driving home	1	SSL A	
P	parking area	2	SSL B	
	emergency stop bay	3	SSL C	
	emergency lane	4	SSL D	
	rightmost lane	5	SSL E	
	current lane	6	SSL F	
	emergency braking	7	SSL G	

Fig. 5. Prioritization of safe state locations (SSL).

A. *Safe State Locations*

In case of normal or failure conditions, a defined driving cycle must be completed and the vehicle must be transitioned to a safe state. Depending on the current system state, different scenarios can be used for transitioning the vehicle to a standstill. Regarding the aspect of safety and availability, the best case scenario for transitioning the vehicle to a standstill would be to proceed driving to the destination set by user/passenger. Based on predicted values for the energy resources and the total energy demand for driving to the destination set by user, the EMS tries to allocate the energy resources in a way that the driving cycle can be completed. If no solution is found, the driving destination must be adapted for reducing the energy demand. The next safest driving destination with reduced energy demand could be for example a parking area. As illustrated in Fig. 5, the driving destinations used by the EMS are prioritized according to the safety and availability aspect. Driving home is considered to be the best case scenario, a sudden emergency braking in the same driving lane the worst case scenario.

Depending on the current system state, the best possible scenario will be selected by the EMS. Scenarios for driving to the destination SSL A to SSL E require an operational propulsion, braking and steering function. Depending on the driving environment, destination SSL E could be also reached by coasting without operational propulsion. For executing the scenario SSL F, an operational braking and steering function is required. If no steering function is available, an emergency braking in the same driving lane must be executed. Furthermore, it is assumed that all sensors and logic required for executing the transition to a safe state are functional. If not, the choice of the safe state location can be also adapted to the state of the sensing and logic functions.

B. *Levels of the Degradation Concept*

If the energy resources are greater than the total energy demand for completing a driving cycle, then no degradation is

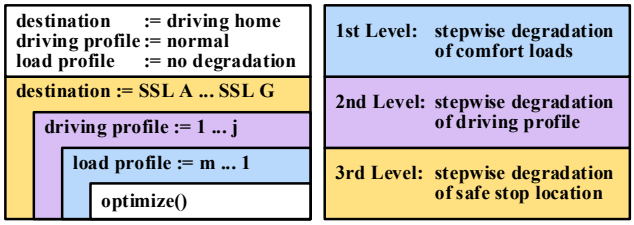

Fig. 6. Schematic program sequence of 3-level-degradation concept.

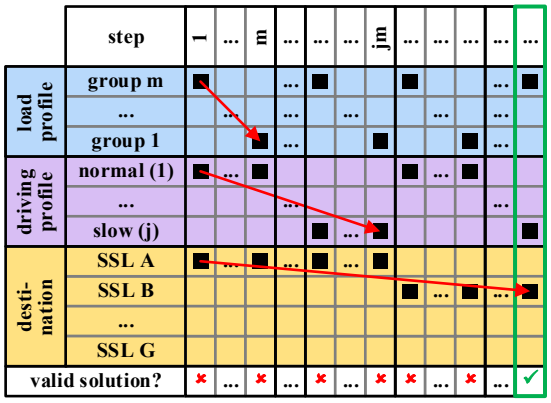

Fig. 7. Schematic process of 3-level-degradation concept.

done. The task of the EMS is in this case only the energy flow optimization for increasing the overall efficiency.

If the energy resources are not sufficient for completing a driving cycle, a degradation concept is required for reducing the total energy demand. A 3-level-degradation concept is used by the EMS presented in this work. As illustrated in Fig. 6, the three levels are in particular degradation of comfort loads, of driving profile and of safe stop destination.

On the first level of the degradation concept, the energy demand of comfort loads will be reduced stepwise. Each Sub EMS stores a look-up table containing the assignment of comfort loads to different groups. Such a partitioning of loads into groups is also proposed in [13]. For the generic EMS, it is assumed that the degradation table has up to m groups. Starting with the group m and ending with group 1, the loads will be degraded stepwise. After each degradation step, the control algorithm checks if a valid solution satisfying the energy balance for each sub power net for the duration of the driving cycle exists. If not, the degradation of comfort loads will be proceeded.

If all comfort loads are degraded and still no solution satisfying the energy balance for each sub power net exists, the degradation on the second level containing the driving profile will be executed. It is assumed that up to j different driving profiles regarding velocity and acceleration are stored in the Top EMS. By degrading the driving profile stepwise, the amount of the energy needed for propulsion will be reduced.

If it is still not possible to achieve a valid solution satisfying the energy balance for each sub power net by degrading on first and second level, then the driving destination must be degraded for shortening the distance. The execution of the pseudo code of 3-level-degradation concept as illustrated in Fig. 6 is exemplified in Fig. 7.

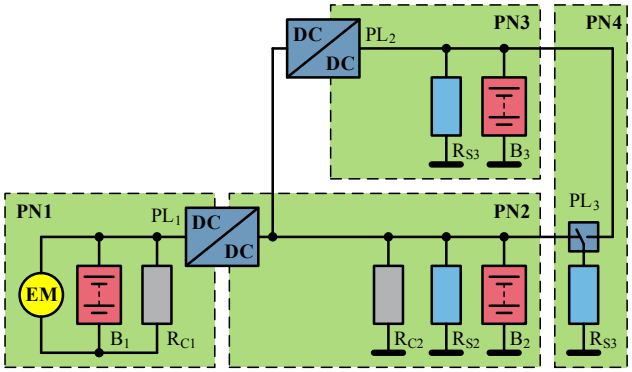

Fig. 8. Assumed power net topology for automated driving.

The control strategy starts the energy flow optimization with initial values for load profile (no degradation), driving profile (normal velocity and acceleration) and for driving destination (as set by the user/passenger). Since no valid solution exists for this step, the control strategy first tries to achieve the energy balance by degrading stepwise the m groups of comfort loads, then subsequently by degrading the driving profile and destination. As illustrated in Fig. 7, a valid solution is found for destination SSL B with a slow driving profile and all degraded comfort loads. The control of components as well as the changes in the driving profile and destination are only activated after a valid solution is found. This degradation concept can also be easily adapted to the preferences of the vehicle manufacturers if any degradation level is required in another form or not at all.

VII. Example of Energy Flow Optimization

The application of the EMS presented in this work will be exemplified in this Section on the power net topology based on the work presented in [2, 3] and illustrated in Fig. 8. An additional sub power net 4 with a toggle switch is added to the topology.

The assumed topology consists of four sub power nets. Sub power net 1 is supplied by the high voltage battery (B_1) and has propulsion (electrical machine EM) and comfort components (R_{C1}). Low voltage sub power net 2 (PN2) is supplied by sub power net 1 (PN1) via a DC/DC converter (PL_1), assumed to be operational in forward (energy flow from power net 1 to 2), reverse (from 2 to 1) or off mode. Sub power net 2 has a low voltage battery (B_2), comfort (R_{C2}) and safety-critical components (R_{S2}). Low voltage sub power net 3 (PN3) is supplied via DC/DC converter (PL_2) from PN2. It is also assumed that PL_2 is operational in three modes: forward (energy flow from sub power net 2 to 3), reverse (from 3 to 2) and off mode. Low voltage sub power net 4 (PN4) can be supplied via a toggle switch (PL_3) either from sub power net 2 (mode net2) or 3 (mode net3). So, in total 18 (3*3*2) operational points are possible.

Furthermore, the predicted values for the available energy resources ($E_{bat\{i\}}$) and demands ($E_{load\{i\}}$) as well as energy flow efficiencies are as illustrated in Fig. 9.

According to the definition made in Section V (4), the sub power nets 1 and 3 are classified as sources (marked green in

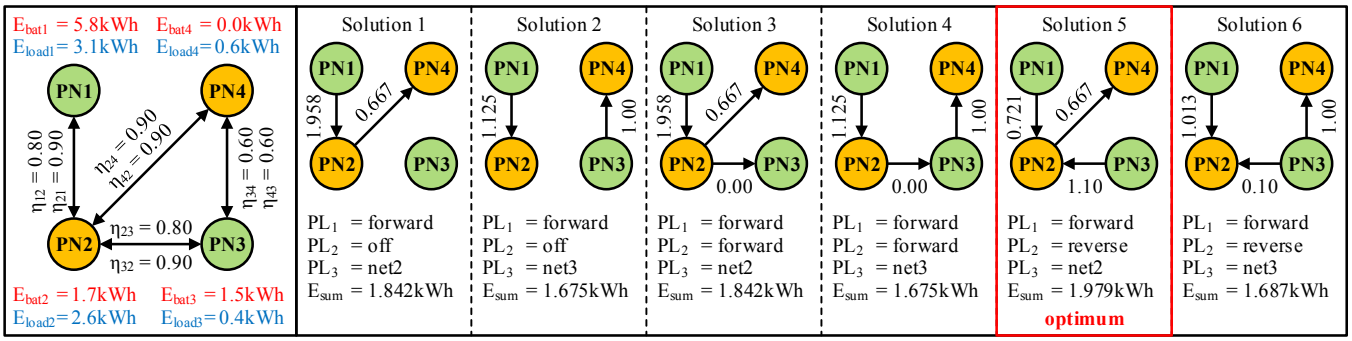

Fig. 9. Assumed power net system state and possible solutions for energy flow optimization problem.

Fig. 9). The sub power nets 2 and 4 are classified as sinks, since their energy demand is higher than available energy resources (marked orange in Fig. 9). From 18 possible operating points only 6 are a valid solution for the energy flow optimization problem satisfying the energy balance in all four sub power nets, which are illustrated in Fig. 9. Out of this 6 possible solutions, solution 5 will be chosen by the EMS, since the remaining energy E_{sum} after completing a driving cycle is maximum at this solution. The energy flow is then controlled by the EMS.

VIII. Conclusion

The EMS presented in this work is based on a generic control strategy concept developed for fail-operational, distributed power nets used for automated driving. The generic concept is adapted to a specific vehicle power net via configuration files, so no new development is required for different topologies. An appropriate system architecture of the EMS was presented.

A control strategy based on the theory of optimal control was considered to be best suited for implementing an adaptive and real-time control algorithm guaranteeing reliable power supply in both, normal and failure case operations. Distributed power net topologies consisting of up to n ($n \geq 1$) sub power nets were mathematically modeled for defining an appropriate cost function and system constraints needed for formulation of the energy flow optimization problem based on predicted values for energy resources and demands for completing a driving cycle. The goal of the defined optimization problem is to find an optimal solution satisfying the energy balance condition for all functional sub power nets while maximizing the overall system energy flow efficiency. An appropriate matrix and vector based system representation needed for implementing the real-time energy flow optimization problem was developed.

Satisfying the energy balance condition means to guarantee that the overall system energy demand can be covered with available energy resources. For the case that no solution exists, a 3-level-degradation concept was proposed for adapting the total system energy demand to available power net resources. The main goal of the implemented degradation concept is to enable a vehicle safe stop at the safest possible destination by using the best suited driving profile regarding velocity and acceleration with the maximum of comfort possible at the current system state. Finally, the application of the energy flow optimization was exemplified for a given power net topology used for automated driving.

References

[1] *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, SAE International Standard J3016 SEP2016, 2016.

[2] J.-L. Augier, T. Huck, A. Kilic and W. Müller, "Efficient, Safe and Reliable Powernet for AD," in *Elektrik/Elektronik in Hybrid- und Elektrofahrzeugen und elektrisches Energiemanagement VII*, Renningen, expert verlag, 2016, pp. 398-411.

[3] A. Kilic and W. Müller, "Fehlertolerante Bordnetze für autonomes Fahren," in *4. Internationaler Fachkongress Bordnetze im Automobil*, Ludwigsburg, 2016.

[4] M. Roth, "Betriebsstrategie," in *Energiemanagement im Kraftfahrzeug - Optimierung von CO2-Emissionen und Verbrauch konventioneller und elektrifizierter Automobile*, Wiesbaden, Springer Vieweg, 2014, p. 323.

[5] L. Guzzella and A. Sciarretta, "Supervisory Control Algorithms," in *Vehicle Propulsion System - Introduction to Modeling and Optimization*, 3rd ed., Berlin Heidelberg, Springer, 2013.

[6] T. Radke, "Energieoptimale Längsführung von Kraftfahrzeugen durch Einsatz vorausschauender Fahrstrategien," Ph.D dissertation, Dept. Mech. Eng., Karlsruhe Institute of Technology, Karlsruhe, 2013.

[7] J. von Grundherr, "Ableitung einer heuristischen Betriebsstrategie für ein Hybridfahrzeug aus einer Online-Optimierung," Ph.D. dissertation, Dept. Mech. Eng., Technical University of Munich, Munich, 2010.

[8] A. Kleimaier, "Optimale Betriebsführung von Hybridfahrzeugen," Ph.D. dissertation, Dept. Elect. Eng., Technical University of Munich, Munich, 2003.

[9] H.-G. Wahl, "Optimale Regelung eines prädiktiven Energiemanagements von Hybridfahrzeugen," Ph.D dissertation, Dept. Mech. Eng., Karlsruhe Institute of Technology, Karlsruhe, 2015.

[10] T. Salcher, "Optimierte Betriebsstrategie hybrider Antriebssysteme für den Serieneinsatz," Ph.D. dissertation, Dept. Elect. Eng., Technical University of Munich, Munich, 2012.

[11] A. Wilde, "Eine modulare Funktionsarchitektur für adaptives und vorausschauendes Energiemanagement in Hybridfahrzeugen," Ph.D dissertation, Ph.D. dissertation, Dept. Elect. Eng., Technical University of Munich, Munich, 2009.

[12] M. Back, "Prädiktive Antriebsregelung zum energieoptimalen Betrieb von Hybridfahrzeugen," Ph.D. dissertation, Dept. Elect. Eng., University of Karlsruhe, Karlsruhe, 2005

[13] A. Basler, "Eine modulare Funktionsarchitektur zur Umsetzung einer gesamtheitlichen Betriebsstrategie für Elektrofahrzeuge," Ph.D dissertation, Dept. Mech. Eng., Karlsruhe Institute of Technology, Karlsruhe, 2015

[14] *Road vehicles – Functional Safety – Part 3: Concept phase*, ISO International Standard 26262-3, 2011.