

# Chapter 55

## Functional Safety System Design on EPS

Zhihong Wu, Xiezu Su, Yuan Zhu and Luke

**Abstract** This paper aims to present the safety design and analysis method complied with ISO 26262 based on EPS (Electric Power Steering) application. There are six sections included in this paper. At the first section, it introduces the functional safety basic idea for risk reduction and the work principle of pinion-EPS. Then the hazard analysis and risk assessment of EPS system is carried out which is significant for the concept stage of functional safety. With HARA (Hazard Analysis and Risk Assessment) result, safety goal and safety requirement are derived, and also the safety mechanism is designed. To verify the plausibility of safety mechanism design, a failure analysis is conducted to perform as evidence for safety case report. The failure analysis is finished by means of FMEDA and PMHF. And as innovative part of this paper, a Markov model for safety path is created and the qualitative analysis is applied. Last but not the least, a conclusion of the paper is finished on the sixth section.

**Keywords** Functional safety · Safety concept · Safety analysis · Markov method · EPS

---

Z. Wu · X. Su (✉)  
School of Automotive Engineering, Tongji University, Shanghai, China  
e-mail: [suxiezu@126.com](mailto:suxiezu@126.com)

Z. Wu  
e-mail: [zhihong.wu@tongji.edu.cn](mailto:zhihong.wu@tongji.edu.cn)

Z. Wu · Y. Zhu · Luke  
Sino-German School for Postgraduate Studies, Tongji University, Shanghai, China  
e-mail: [yuan.zhu@tongji.edu.cn](mailto:yuan.zhu@tongji.edu.cn)

Luke  
e-mail: [luke@tongji.edu.cn](mailto:luke@tongji.edu.cn)

### 55.1 Introduction for EPS System & Functional Safety

Functional safety related with ISO 26262 in automotive is a hot topic for researchers these days. Some papers focus on ASIL decomposition algorithm investigation [1–3]. These three papers translate ASIL allocation and decomposition task to different mathematical models which make the components ASIL allocation automatically. Paper [4] presents the hazard analysis techniques which is very important for concept stage. Paper [5] covers the safety case report from customer points of view. Paper [6] writes about safety mechanism which is critical for functional safety. However, all these papers either describe functional safety in a theoretical way or just offer partial solution for functional safety. This paper tries to present the complete methodology for functional safety based on electrical power steering application which makes the reader understand the standard much easier.

Electric power steering is a typical critical safety item for vehicle. The functional safety requirement for EPS is originally from car maker. To initialize the lifecycle of functional safety development, the system function should be known. For EPS system, the driver firstly input the steering command from the steering wheel and this input is captured by the torque sensor which will feed the signal into MCU (Micro Control Unit). Besides, other system related signals such as wheel steering angle, vehicle speed, environmental temperature and battery voltage are also feed into MCU. The software’s main functional tasks are calculating the motor output torque and motor control regulation. The torque is calculated based on kinds of sensor signals as stated before, road condition and related steering strategies. This calculated motor torque is the reference input of motor vector control regulation with FOC algorithm. And finally the torque output by the motor will force the steering system to work correctly. Figure 55.1a shows the hardware architecture of two pinions EPS system.

The target for functional safety is about to reducing the risk of harm by kinds of failure to a safe level. As Fig. 55.1b shows, there are residual risk, tolerable risk and inherent process risk. The safe level of risk is to reducing the harm risk to tolerable level. The so called residual risk is the risk that no safety mechanism covers. The

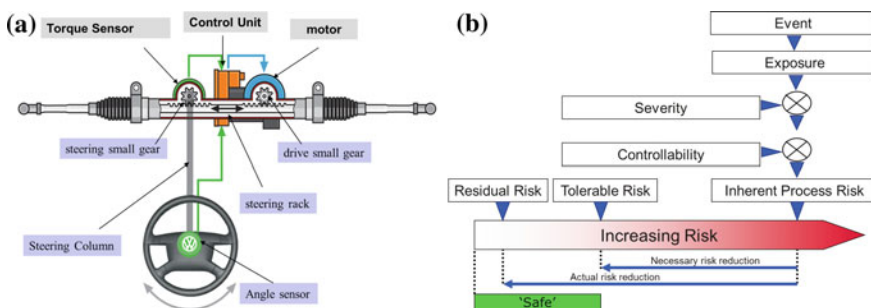


Fig. 55.1 a P-EPS hardware architecture b Risk reduction for ISO 26262

inherent process risk is brought by events that happen in specific scenario and it is necessary to be reduced by safety mechanism. According to safety requirement, the risk reduction by safety measures (actual risk reduction) should be more than the risk that the hazard brought in (necessary risk reduction). The risk level is evaluated in the HARA phase which will be detailed in the next section.

Since ISO 26262 only deals with electric and electronic system, the EPS E/E system is presented as Fig. 55.2. This item contains elements like sensors, safety power supply, safety MCU, safety driver, MOSFET B6, load switch and anti-polarity circuit, phase separation unit and also CAN bus network. Since the malfunctions of the item will be allocated into the elements failure modes in the FMEDA report, then each element’s failure modes should be carefully checked and classified.

Functional safety is not only about product design but also goes through all the production procedures. The lifecycle of functional safety is involved in the implementation of safety-related systems and it starts at the concept phase of a project and finishes when all of the E/E/PE safety-related systems and other risk reduction measures are no longer available for use [8–10].

Noted from the functional safety life cycle block diagram as showed in Fig. 55.3a [1], the concept phase is the starting stage of the lifecycle which contains item definition, initialization of safety lifecycle, HARA and functional safety concept. Among the four parts of the concept phase, HARA is the most important one. One work product for HARA is deriving safety goals which are important inputs for functional safety concept.

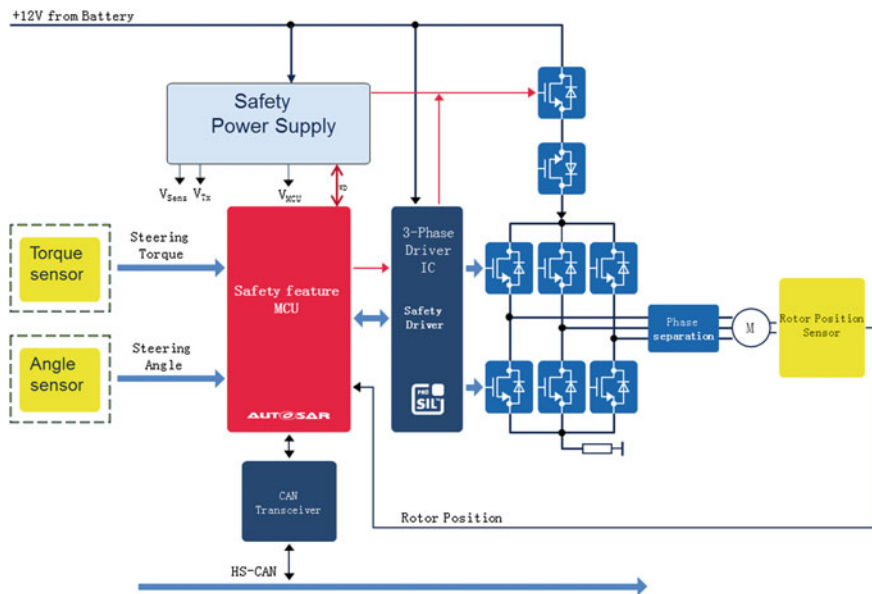


Fig. 55.2 PMSM EPS topology

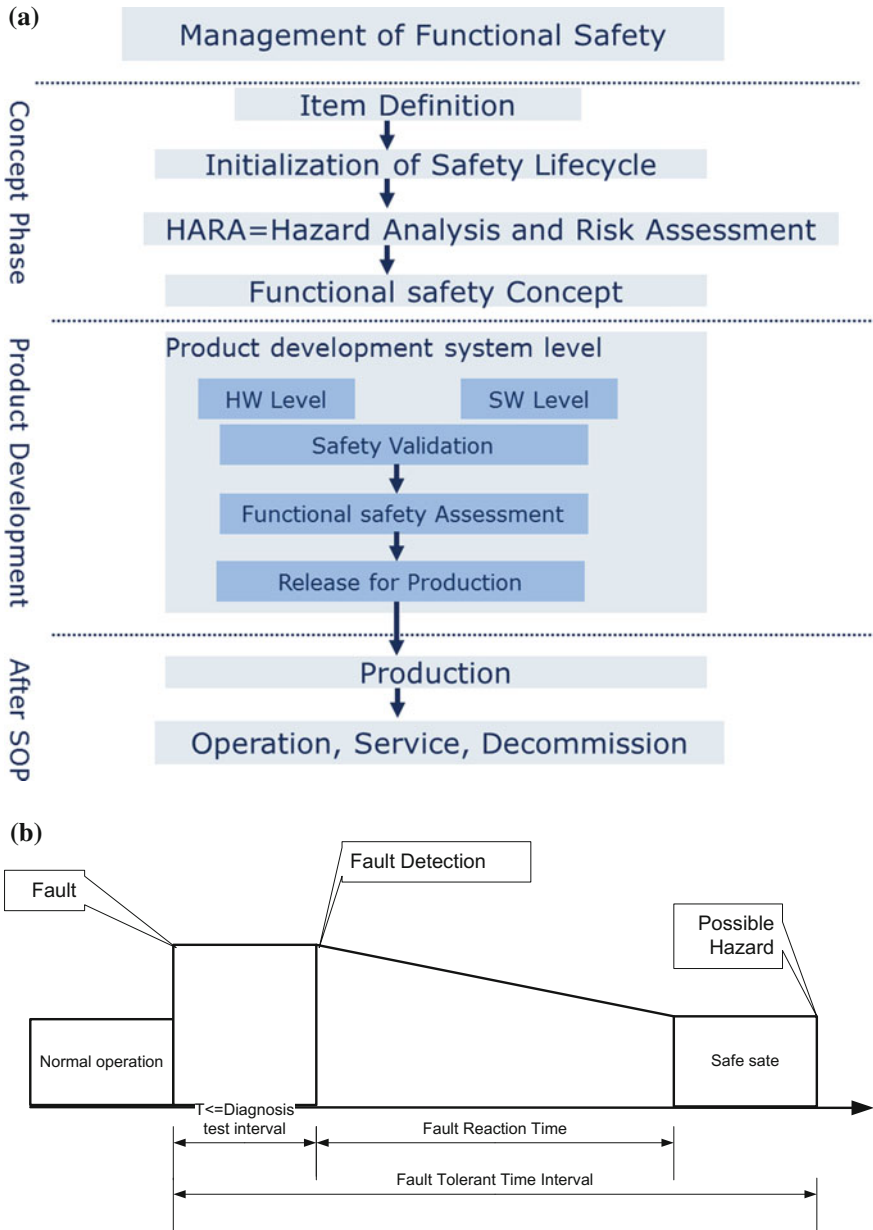


Fig. 55.3 a Functional safety life cycle b FTI block diagram

## 55.2 Hazard Analysis and Risk Assessment

The main task of HARA is classifying hazard which caused by malfunction of the item into different risk levels based on the severity of hazard (S), the exposure probability (E) and the controllability to avoid the harm (C). The combination of ‘SEC’ will result in five different hazard levels as QM, ASIL A, ASIL B, ASIL C and ASIL D. Each hazard will be assigned a SG (Safety Goal) and the SG shares the same ASIL rating as hazard. The safety goal is the top safety requirement of the system, and is realized by the combination of correct function and properly safety mechanism. The ASIL rating is directly related with the developing complexity and developing resources. Generally speaking, the ASIL C and ASIL D level demands considerable more resources than ASIL B and ASIL A. Thus, over rating of the ASIL level is not recommended for cost and technique reasons.

As for EPS application, the HARA result is briefly introduced as Table 55.1. The complete HARA contains more content than this table. Here the ASIL allocation part is kept and presented. Take the malfunction of ‘blocked steering’ for instance, if it happened the steering would not available. And this hazard may cause the vehicle be collided which will cause serious injure even death, so ‘S3’ is assigned. This hazard could happen at all driving situation, thus the probability of the hazard is high which means ‘E4’. Last but not least, the vehicle could not be controlled if the hazard happened. Thus, ‘C3’ is allocated to this hazard. According to ISO 26262, the combination of S3, E4 and C3 makes the item ASIL level to be D. Other malfunction can be analyzed similarly. As Table 55.1 shows, the final item ASIL rating follows up the highest one, which is ASIL D.

**Table 55.1** Hazard analysis and risk assessment for EPS application

Malfunction	Hazard	S	E	C	‘SEC’ comment	ASIL
Erratic EPS	Turning not accurate	S2	E4	C2	Steering possible but need high skill; it can happen at all driving situation; drivers have to react fast to adapt to new steering performance.	B
Sudden EPS loss	Turning mechanically	S0	E4	C1	Vehicle can be controlled	QM
Sudden EPS reactivation	Turning assist normally	S0	E4	C1	Vehicle can be controlled	QM
Self steering	Turning automatically	S3	E4	C3	Steering impossible will cause serious injure; it can happen at all driving situation; impossible to control the vehicle	D
Blocked steering	Turning impossible	S3	E4	C3	Steering impossible will cause serious injure; it can happen at all driving situation; impossible to control the vehicle	D

**Table 55.2** Safety goal on EPS application level

ID	Safety goals	ASIL	Safety state
APP-SG-01	Self-steering less than 20 ms	ASIL D	Switch and keep off min. 5 FETs
APP-SG-02	Blocked steering less than 100 ms	ASIL D	Switch and keep off min. 5 FETs
APP-SG-03	Erratic support of steering assist less than 100 ms	ASIL B	Switch and keep off min. 5 FETs
APP-SG-04	Sudden loss of steering assist	QM	Switch and keep off min. 5 FETs
APP-SG-05	Sudden reactivation of steering assist	QM	Switch and keep off min. 5 FETs

**Table 55.3** Safety requirement on MOSFET driver [7]

ID	Functional safety requirement	ASIL	Corresponding SG
DR-SR-01	Two or more FETs unintended 'on' less than 100 ms	ASIL D	APP-SG-02
DR-SR-02	Protect $\mu\text{C}$ against destruction when driver IC damaged	ASIL D	Not derived from SG
DR-SR-03	Undetected wrong current measurement (>20%)	ASIL B	APP-SG-03
DR-SR-04	Protect driver against destruction when $\mu\text{C}$ damaged	ASIL D	Not derived from SG
DR-SR-05	Unwanted activation of phase separation	QM	APP-SG-04

### 55.3 Safety Goal and Safety Requirement

As stated above, safety goals are derived from hazard analysis and risk assessment. Corresponding to the hazard analysis and risk assessment, the safety goal is listed as Table 55.2. One of the important parameters that matters a lot in the product development is the FTTI (fault tolerant time interval) as Fig. 55.2b shows. FTTI means that a time slot starts at fault happens and ends at possible hazard starts. For functional safety, the system should have entered into safety state within FTTI. FTTI is usually acquired by theory calculation on vehicle model and practical vehicle test, especially road test. Normally, it is offered by OEM. This system parameter can be independently pointed out or be integrated into safety goals. In this paper, the latter method is chosen. Different OEMs or Tiers may describe their safety goals differently, but the meaning behind the word should be the same.

Safety requirements are derived from safety goals. Different elements may have different safety requirements for certain safety goals. In other words, some elements' failure may not result in the violation of certain safety goals while some ones may result in safety goals violation. Take EPS MOSFET driver for example, the functional safety requirements are list as Table 55.3. Most safety requirements are allocated to related elements by FTA (fault tree analysis) method. Safety goal is

the reverse of the top event of fault tree, while safety requirements for each element are reverses of bottom events of fault tree. The fault tree number is as the same as safety goals number. Each safety goal has its fault tree respectively.

## 55.4 Safety Concept

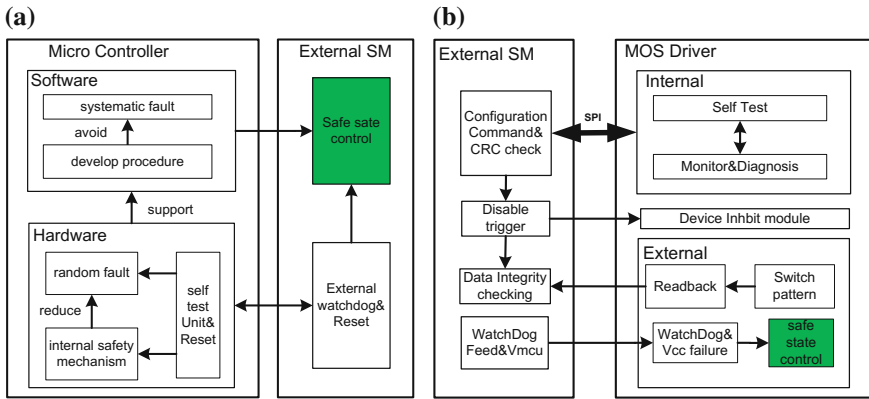
Safety concept is the theory, method and technology that make the system enter into safety state or avoid the hazard happen. Safety state means that no hazard will happen. The hazard if happened would violate the safety goals, thus the system should enter into safety state for functional safety purpose. For EPS application, the safety state for all safety goals is switching off the motor current which means shutting down the inverter or enabling the phase cutting off unit. Safety mechanism is part of safety concept which implements the safety requirement. By safety mechanism, the risk of hazard will be reduced to acceptably low.

There are three key elements in EPS E&E system as power supply, micro-controller and MOSFET driver (also called pre-driver). The safety requirements for these three elements are derived from safety goals. As stated above, the EPS E&E system is rated as ASIL D level. Thus, the safety requirements for power supply, micro controller and pre-driver are also ASIL D level. However, that does not mean every part of the elements should be ASIL D but only safety related.

The purpose of the safety mechanism can be made into three parts: 'safe acquisition', 'safe calculation' and 'safe actuation'. 'Safe acquisition' means the sensor information is correct. Sensor is relative simple compared with micro controller and MOSFET driver. The usual way to make safe acquisition is redundancy which means two sensors are used for one signal sense.

'Safe calculation' means the micro controller works correctly, see as Fig. 55.4a. There are three things need to be considered for 'safe calculation': operational condition; random hardware fault; software fault. Operational condition is mainly about power supply, temperature etc. The random hardware fault for micro controller is about soft fault and hard fault. Soft fault is related with memory data transient transition, like '0' change to '1'. Hard fault is permanent fault, e.g. GPIO stuck at '1'. The software fault is systematic fault. It can be avoided by correct developing procedure. The random hardware is not avoidable but only reduced. It is protected by internal safety mechanism (e.g. lockstep CPU) and the internal safety mechanism is monitored by self-test unit. However, the internal safety mechanism and self-test may be malfunction during worst work condition, e.g. over voltage, under voltage, over temperature. Thus, external safety mechanism is applied on micro controller.

'Safe actuation' means the MOSFET driver can output correctly according to the input and can be shut down at failure situation, shown as Fig. 55.4b. The MOSFET driver contains functional units such as charge pump and sub power supply. Their failure modes such as over temperature, over-voltage and under-voltage should be monitored by safety mechanism. And the MOSFET failure modes should also be



**Fig. 55.4** a Safe calculation concept diagram b Safe actuation concept diagram

diagnosed such as short to GND or short to battery by safety mechanism. All these safety mechanism is also monitored by self-test unit. These safety mechanisms are referred as internal safety mechanism. And they can be configured by a safe SPI interface (CRC check applied). What’s more, the switch pattern need to be checked to guarantee the MOSFETs is switched as the software commands. Thus an independent read back loop from MOSFETs are integrated. Then the read back result can be compared with the original switching command. If not the same, the micro controller can inhibit the MOSFET driver which makes the system into safe state. A watchdog is also integrated for monitoring the MCU. The watchdog feed failure or MCU supply Vcc failure will trigger the safe state control active which will output a signal to cut off the motor phase current.

As functional safety focuses on E/E system, all parts need power supply. Then, ‘safe supply’ should be included in the safety concept. The basic safety function for the supply IC is detecting under voltage and overvoltage failure events in supplying the attached elements (MCU, sensors, and transceiver), and generates the reset or interrupt signals as configured. It shall also read the hardware status of MCU, which indicates on ERR pin of MCU. What’s more, the supply IC shall monitor the microcontroller software operation by means of watchdog and it shall provide a Safe State Control (SSC) capability in case the watchdog feed failure. The whole safety mechanism is presented as Fig. 55.5 considering safe supply, safe calculation, safe actuation and safe acquisition.

### 55.5 Safety Analysis

The main task of safety analysis is to examine the consequences of faults and failures on the functions, behavior and design of items and elements and check target safe state is achieved or not. Safety analysis is not only able to verify the



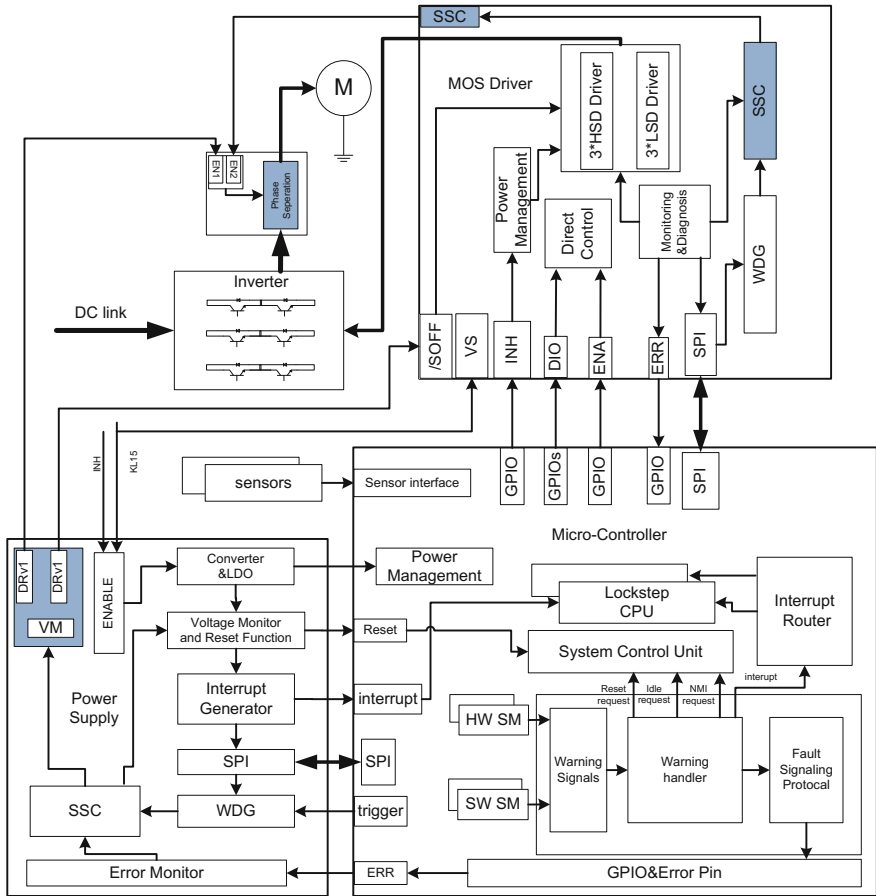


Fig. 55.5 Safety mechanism block diagram

Table 55.4 Single point fault metric for ASIL ratings

	ASIL B	ASIL C	ASIL D
SPFM	≥ 90%	≥ 97%	≥ 99%

Table 55.5 Latent fault metric for ASIL ratings

	ASIL B	ASIL C	ASIL D
LFM	≥ 60%	≥ 80%	≥ 90%

safety concept but also can correct the defect part of the preliminary safety design. Safety analysis is a dynamic process. It should be done from the concept phase to the development phase; thus it will be updated frequently. Safety analysis can be performed on different level of abstraction such as item level or element level (system, hardware, software) (Tables 55.4 and 55.5).

FMEDA is the typical quantitative method for safety analysis, which means failure mode effect and diagnostic analysis. FMEDA is a powerful tool that it can be used for different levels analysis such as system, sub system, component, component part etc. The key point for FMEDA is making a worksheet according to ISO 26262 requirement. Normally, the FMEDA format is changeable, but the FMEDA need to cover failure rate related with dedicated failure mode (also failure distribution and classification, for example microcontroller has permanent and transient failures), the safety mechanism that mitigates the hazard and the required hardware metrics as residual or single point fault metric and latent fault metric for the failure mode. FMEDA is the IP of the designer for functional safety and usually it is confidential. Table 55.6 is an example of the FMEDA. For real application, the FMEDA need consider each part of the hardware design. It performs as an important rational to support the functional safety argument. Sometimes, the FMEDA is made up with two parts as FMEA (failure mode and effect analysis) and DC (diagnosis coverage) worksheets.

Different ASIL rating level item requires different quantitative specifications. According to ISO 26262, there are two kinds of hardware evaluation parameters which are hardware architectural fault metrics and random hardware failure rate. The hardware architectural fault metrics contains single point fault and latent fault metrics which are integrated into FMEDA. The definition of SPFM and LFM are list as Eq. 55.1 and Eq. 55.2.

$$SPFM = 1 - \frac{\sum_{SR,HW} (\lambda_{SPF} + \lambda_{RF})}{\sum_{SR,HW} \lambda} = \frac{\sum_{SR,HW} (\lambda_{MPF} + \lambda_S)}{\sum_{SR,HW} \lambda} \quad (55.1)$$

$$LFM = 1 - \frac{\sum_{SR,HW} (\lambda_{MPF,L})}{\sum_{SR,HW} (\lambda_{MPF} + \lambda_S)} = \frac{\sum_{SR,HW} (\lambda_{MPF,DP} + \lambda_S)}{\sum_{SR,HW} (\lambda_{MPF} + \lambda_S)} \quad (55.2)$$

Notes:

SPF	single point fault;
RF	residual fault;
MPF	multi-point fault;
S	safe fault;
SR	safety related;
MPF, L	latent multi-point fault;
MPF, DP	detected or perceived multi-point fault.

The fault metrics requirements for different ASIL levels are contained in Table 55.6.

The other parameter that needs to be calculated is the system random hardware failure rate. ISO 26262 suggests the method of using a probabilistic metric called “Probabilistic Metric for random Hardware Failures” (PMHF) to evaluate the violation of the considered safety goal. As stated in ISO 26262, if the fault point number is more than three, then the fault is considered to be safe multipoint fault

**Table 55.6** FMEDA example

Component	Sub-part	Safety related?	Failure mode	Failure rate	SM preventing SG violation	Failure mode coverage wit. SG violation	Residual or singles point fault failure rate	SM preventing latent fault	Failure mode coverage wit. Latent failures	Latent fault failure rate
Pre-driver	Power supply	SR	S2G	20	SM1	70%	6	SM1	90%	$(20-6) * 10\% = 1.2$
	...		...							
Safety mechanism	SM1	SR								
	...									
							Total single point failure rate: xxx			Total latent failure rate: xxx
							SPFM: XXX			LFM: XXX
							Total failure rate: xxx			
							Total Safety Related: xxx			
							Total Not Safety Related: xxx			

**Table 55.7** PMHF for ASIL ratings

	ASIL B	ASIL C	ASIL D
PMHF	$<10^{-7}h^{-1}$ or $< 100FIT$	$<10^{-7}h^{-1}$ or $< 100FIT$	$<10^{-8}h^{-1}$ or $< 10FIT$

**Table 55.8** Failure rates for ‘blocked steering’

Name	Parameters	Failures for ‘blocked steering’
Total failure rate	$\lambda$	51.3 FIT
Safe faults	$\lambda_s$	21.9 FIT
Single point and residual faults	$\lambda_{SPF} + \lambda_{RF}$	0.3 FIT
Detected multiple point faults	$\lambda_{MPF,D}$	26.3 FIT
Latent multiple point faults	$\lambda_{MPF,L}$	2.8 FIT
Not safety related faults	$\lambda_{NSR}$	35.9 FIT
Single point fault metric	SPMF	99.5%
Latent fault metric	LFM	94.5%
Probabilistic metric for random hardware failures	PMHF	0.3 FIT

unless other evidence is provided. Thus, PMHF only consider the single point fault and the dual point fault. Usually, a mission block is monitored by safety mechanism. The failure of safety mechanism should be considered when evaluating the failure of the mission. And the calculation method is carried on as Eq. 55.3 stated. The target of different ASIL level hardware failure rate is as Table 55.7. The total failure result is shown as Table 55.8, taking ‘blocked steering’ as an example. The SPMF, LFM and PMHF of ‘blocked steering’ are all located in ASIL D range

$$M_{PMHF} = \lambda_{m,RF} + \frac{1}{2} \lambda_{m,DPF} (\lambda_{sm,RF} + \lambda_{sm,DPF,latent}) T_{lifetime} \tag{55.3}$$

Notes:

- m, RF                      residual fault of mission block;
- m, DPF                     dual point fault of mission block;
- sm, RF                     residual fault of safety mechanism;
- sm, DPF, latent         latent fault of safety mechanism.

### 55.6 Markov Analysis for Safety Path

Safety path (short as SP) means a signal loop that makes the item enter into safety state. As for EPS application, the signal will trigger the phase separation module or shutting down the power supply. The safety path is very significant for system safety. If safety path is failed, the safety state cannot be reached when there is item

malfunction. For functional safety purpose, one safety path is not safe enough. The common way is to offer at least two safety paths to achieve ASIL D functional safety rating. These two safety paths should be independent with each other. Hereafter, the safety paths for EPS system are presented. There are three main parts in the EPS control unit which are power supply, micro-controller and MOSFET driver. Each device is possible to trigger the safety path. There are three implementation topologies for safety path as Fig. 55.6 shows. The basic idea of the safety path is to activate the phase separation unit or cut off the power supply of the power stage which makes the motor stop running. Then power steering is lost when enter into safe state and only manual steering is possible.

- Safety path by supply and driver, as showed in Fig. 55.6a. SP1 is triggered by safety power supply safety mechanism such as watchdog feeding failure by MCU, over voltage, under voltage, short circuit and over temperature. If these hazards happen, the safety mechanism of power supply will activate the safety path signal. The signal form can be low, high, PWM or PFM etc. SP2 is triggered by safety driver. The trigger command is issued from MCU or the internal mechanism of safety driver. For instance, if the MCU fails to feed the watchdog of safety driver and the MCU supply is under voltage, the safety sate control unit of the driver will be activated. Also there will be short circuit on the MOSFET,

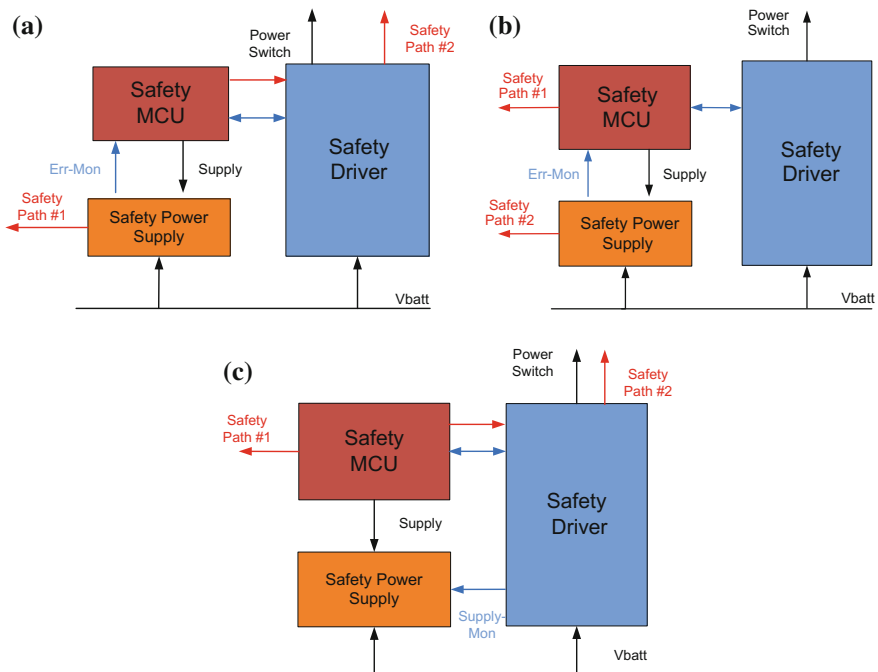
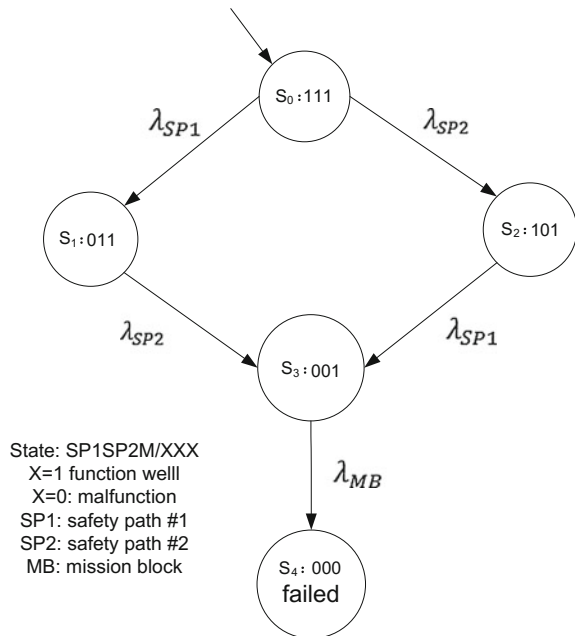


Fig. 55.6 a SP by supply and driver b SP by MCU and supply c SP by MCU and driver

- wrong switching pattern, communication fault alike, all these faults will be sensed by MCU and MCU will trigger the SP2 according to the software strategy.
- Safety path by MCU and supply, as showed in Fig. 55.6b. This scenario is a little different from Fig. 55.6a. The safety driver does not contain safe state control unit to generate the safety path signal for entering into safety state, however other general safety mechanism still exist. Instead, the safety MCU is able to issue a safety path signal directly which will trigger the external module (for EPS, it is phase separation module or power supply load switch) which will make the EPS system into safe state.
  - Safety path by MCU and driver, as showed in Fig. 55.6c. For this scenario, the safety power supply does not generate the safety path signal as previous stated. The two safety paths are implemented by the safety MCU and the safety driver. In this case, the MCU performs significant role for safety path. It not only can trigger the safety path related with safety driver, but also it can independently issue a safety path. However, the SP2 is independent with MCU since the driver has internal mechanism to trigger the SP2 without the involvement of MCU.

As stated before, the safety path concept is critical for the item functional safety. The three safety path topologies for EPS can be modeled by Markov model as Fig. 55.7 shows. Markov model is suitable for system level failure analysis. Three elements need to be considered which are mission block, the first safety path and the second safety path. There is no priority difference between these two safety paths. The system is sentenced to be failed only the three elements are all failed,

Fig. 55.7 Markov chain modeling for safety path



assuming the safety paths is more robust than the mission block. The failure rate of the mission block and safety path can be found in FMEDA and PMHF results.

In order to implement Markov method, you have to define the operating states of the item and figure out the state transfer diagram; then write down the equations according to the state transfer diagram and solve the differential equation. The state failure probability changing rate is decided by the input failure probability changing rate and the output failure probability changing rate. The failure probability changing rate is the product of failure rate and failure probability. And the input flow of the state in state transfer diagram is referred to as positive. And output is negative.

Here we define the EPS system state. We consider SP1, SP2, MB (mission block) and define element function variable  $X_i$  and item state variable  $S_i$  as bellow:

$$X_i = \begin{cases} 1 & \text{if } SP1, SP2 \text{ or } MB \text{ function well} \\ 0 & \text{if } SP1, SP2 \text{ or } MB \text{ malfunction} \end{cases}, i = SP1, SP2, MB$$

$$S_i = X_{SP1}X_{SP2}X_{MB}, i = 0, 1, 2, 3, 4$$

As stated above, SP1 and SP2 are independent with each other. Their failures are also independent with each other. Thus, there are two failure paths as showed in Fig. 55.7. The item's initial state is  $S_0$ , in which safety paths and mission block all works well. Then the item can either run into  $S_1$  or  $S_2$ , with one safety path fails, but the whole system still works. Then the system will run into  $S_3$ , where both safety paths fails, but the mission block still works. Last but not the least, the item will run into failure state, which is  $S_4$ , mission block does not works anymore. The failure rate of safety path #1, safety path #2 and mission block are written as  $\lambda_{SP1}$ ,  $\lambda_{SP2}$ ,  $\lambda_{MB}$ . The Markov chain of the item is illustrated as Fig. 55.7.

The differential equation of the Markov chain is list as bellow. The state  $S_4$  is the system failure state and the calculation of the probability of  $P_{S4}$  is significant for item performance evaluation.

$$\begin{cases} \frac{dP_{S0}}{dt} = -(\lambda_{SP1} + \lambda_{SP2})P_{S0} \\ \frac{dP_{S1}}{dt} = \lambda_{SP1}P_{S0} - \lambda_{SP2}P_{S1} \\ \frac{dP_{S2}}{dt} = \lambda_{SP2}P_{S0} - \lambda_{SP1}P_{S2} \\ \frac{dP_{S3}}{dt} = \lambda_{SP1}P_{S2} + \lambda_{SP2}P_{S1} - \lambda_{MB}P_{S3} \\ \frac{dP_{S4}}{dt} = \lambda_{MB}P_{S3} \end{cases} \quad (55.4)$$

Assume the following:

$$\begin{cases} \lambda_{MB} \neq \lambda_{SP1} \\ \lambda_{MB} \neq \lambda_{SP2} \\ \lambda_{MB} \neq \lambda_{SP1} + \lambda_{SP2} \end{cases}$$

The initial state  $P(0) = [1, 0, 0, 0, 0]$ , then the solutions of  $P_{S4}$  can be found:

$$\begin{aligned}
 P_{S4} = 1 - & \left[ \frac{\lambda_{SP1} + \lambda_{SP2}}{\lambda_{MB} - \lambda_{SP1} - \lambda_{SP2}} - \frac{\lambda_{SP1}}{\lambda_{MB} - \lambda_{SP1}} - \frac{\lambda_{SP2}}{\lambda_{MB} - \lambda_{SP2}} \right] e^{-\lambda_{MB}T} - \frac{\lambda_{MB}}{\lambda_{MB} - \lambda_{SP1}} e^{-\lambda_{SP1}T} \\
 & - \frac{\lambda_{MB}}{\lambda_{MB} - \lambda_{SP2}} e^{-\lambda_{SP2}T} + \frac{\lambda_{MB}}{\lambda_{MB} - \lambda_{SP1} - \lambda_{SP2}} e^{-(\lambda_{SP1} + \lambda_{SP2})T}
 \end{aligned}
 \tag{55.5}$$

Here  $T$  is the lifecycle of item;  $\lambda_{MB}$  is the mission block failure rate;  $\lambda_{SP1}$  is the first safety path failure rate;  $\lambda_{SP2}$  is the second safety path failure rate. Normally, the inequations as bellow are correct for real application since safety mechanism should be more reliable than mission block.

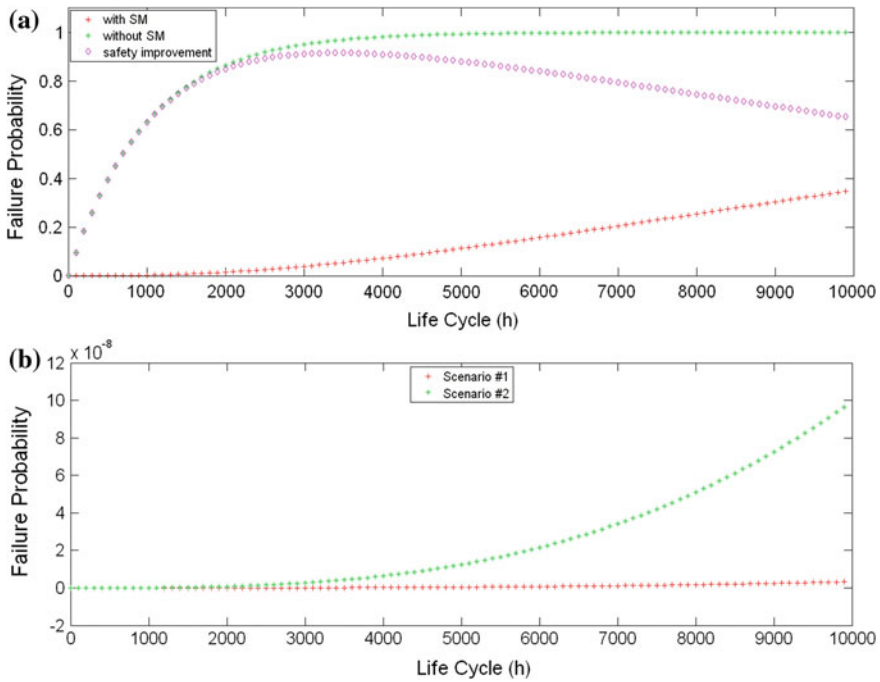
$$\begin{cases} \lambda_{MB} > \lambda_{SP1} \\ \lambda_{MB} > \lambda_{SP2} \end{cases}$$

Considering different failure rate of safety path, two scenarios are considered as Table 55.9 shows. A Matlab program is made to simulate the Markov model. To verify the plausibility of the safety path, a raw failure rate set is chosen  $[\lambda_m, \lambda_{SP1}, \lambda_{SP2}]$  as  $[1E-03/h, 1E-04/h, 1E-04/h]$  on purpose. For reality, the failure rate is much smaller. The reason for choosing this set is to show that although the block mission and the safety path have considerable high failure rate, but the combination of these two ones make the failure rate decrease a lot. Figure 55.8a shows that the safety path makes the safety performance improved a lot for the item lifecycle. The ‘safety improvement’ curve shows that the greatest improvement point happens at the middle range time of the vehicle life cycle. Figure 55.8b indicates that the lower of the safety path failure rate, the more reliable of the system. Scenario #1’s failure probability of the item is greatly decreased compared with scenario #2. It also indicates that scenario #1 is one of failure rate allocation to safety elements to fulfill ASIL D item.

**Table 55.9** Typical values of parameters for Fig. 55.8b

Senario1: $\lambda_m > \lambda_{SP1} + \lambda_{SP2}$		Senario2: $\lambda_m < \lambda_{SP1} + \lambda_{SP2}$	
$\lambda_m$	1E-06/h	$\lambda_m$	1E-06/h
$\lambda_{SP1}$	1E-07/h	$\lambda_{SP1}$	6E-07/h
$\lambda_{SP2}$	1E-07/h	$\lambda_{SP2}$	5E-07/h
T	10 000 h	T	10 00 h





**Fig. 55.8** a Safety path performance evaluation ( $[\lambda_m, \lambda_{SP1}, \lambda_{SP2}] = [1E-03/h, 1E-04/h, 1E-04/h]$ )  
 b Two failure rate scenarios of SP (parameters see Table 55.9)

### 55.7 Conclusion

Functional safety requirement is becoming more and more compulsory these days. What makes safety related item development different is that the item is driven by safety goal. And safety goals of the item are generated from hazard analysis and risk assessment. By achieving the safety goals via V model design method, the risk of harm from item malfunction thus can be decreased to an acceptable low level. To make this argument persuasive enough, safety analysis need to be conducted. This paper proposed safety path concept and fulfilled the safety concept design. And also the item safety performance is investigated by Markov model. The simulation result shows that the safety path improved the item safety a lot even the raw failure rate of the item is somehow large. This paper mainly covers the concept design and hardware evaluation, the principle of system safety software design is the further work direction.

## References

1. Dhoubi MS, Perquis JM, Saintis L, Barreau M (2014) Automatic decomposition and allocation of safety integrity level using system of linear equations. In: The fourth international conference on performance, Safety and robustness in complex systems and applications
2. Mader R, Armengaud E, Leitner A, Steger C (2012) Automatic and optimal allocation of safety integrity levels. In: Proceedings—annual reliability and maintainability symposium (RAMS)
3. Parker D, Walker M etc(2013) Automatic decomposition and allocation of safety integrity levels using a penalty-based genetic algorithm. In: Ali M et al. (eds.): IEA/AIE 2013, LNAI 7906, pp 449–459
4. Baumgart S (2012) Investigations on hazard analysis techniques for safety critical product lines. In: IRSCE'12, Västerås, Sweden, Nov. 11
5. Birch J, Rivett R, Habli I (2013) Safety cases and their role in ISO 26262. In: Functional safety assessment, safety, reliability, and security lecture notes in computer science Vol 8153 pp. 154–165
6. Cherfi A (2014) Modeling automotive safety mechanisms: a markov chain approach reliability engineering and system safety 130 pp. 42–49
7. Infineon internal training notes, 2014
8. ISO: ISO 26262-3 Road Vehicles—Functional Safety. ISO Standard (2011)
9. ISO: ISO 26262-4 Road Vehicles—Functional Safety. ISO Standard (2011)
10. ISO: ISO 26262-5 Road Vehicles—Functional Safety. ISO Standard (2011)