2019 SPID CONFERENCE

AIAG - VDA FMEA Handbook

자동차 산업의 통합된 FMEA 접근법

2019. 09. 26

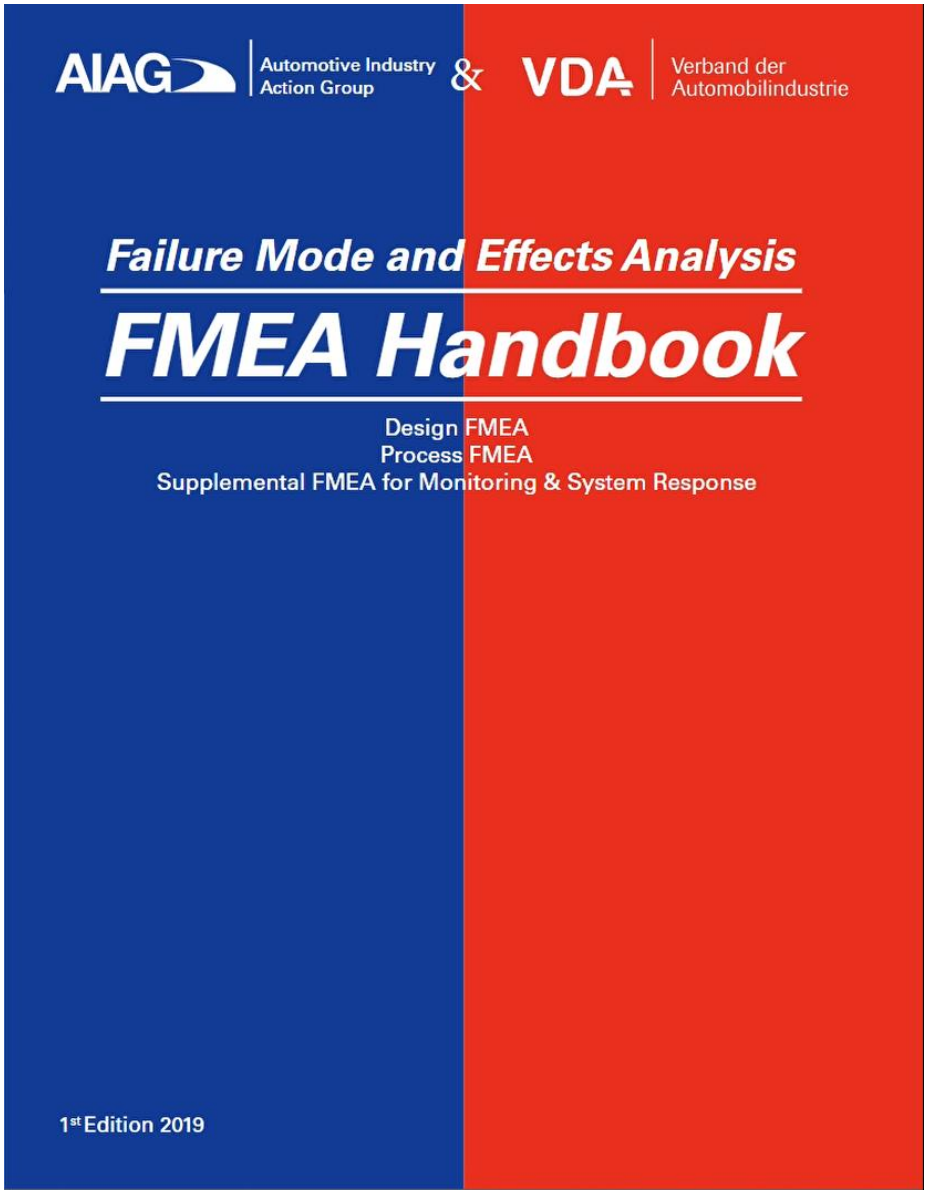
(주)에스피아이디

spid

CMMI Institute Partner

Contents

1. AIAG-VDA FMEA Handbook 소개



1. INTORCUTION
2. EXECUTION OF THE DESIGN FMEA
3. EXECUTION OF THE PROCESS FMEA (PFMEA)
4. SUPPLEMENTAL FMEA FOR MONITORING AND SYSTEM RESPONSE (FMEA-MSR)

APPENDIX

A. SAMPLE FMEA FORM SHEET
B. FORM SHEET - STEP BY STEP HINTS
C. SEVERITY, OCCURRNECE, DETECTION AND ACTION PRIORITY TABLES
D. ADDITIONS
E. FURTHER APPLICATION FIELDS
F. CHANGE POINT SUMMARIES
G. REFFERENCE AND SUGGESTED READING
H. GLOSSARY

1. AIAG-VDA FMEA Handbook 소개

❖ The 7-Step Approach

<New AIAG VDA FMEA Whitepaper
: Improvements, Benefits & Financial Impact of the AIAG & VDA FMEA Handbook-AIAG /2019>

System Analysis			Failure Analysis and Risk Mitigation			Risk Communication
1st Step	2nd Step	3rd Step	4th Step	5th Step	6th Step	7th Step
Planning & Preparation	Structure Analysis	Function Analysis	Failure Analysis	Risk Analysis	Optimization	Result Documentation

❖ Enhanced FMEA Planning & Preparation

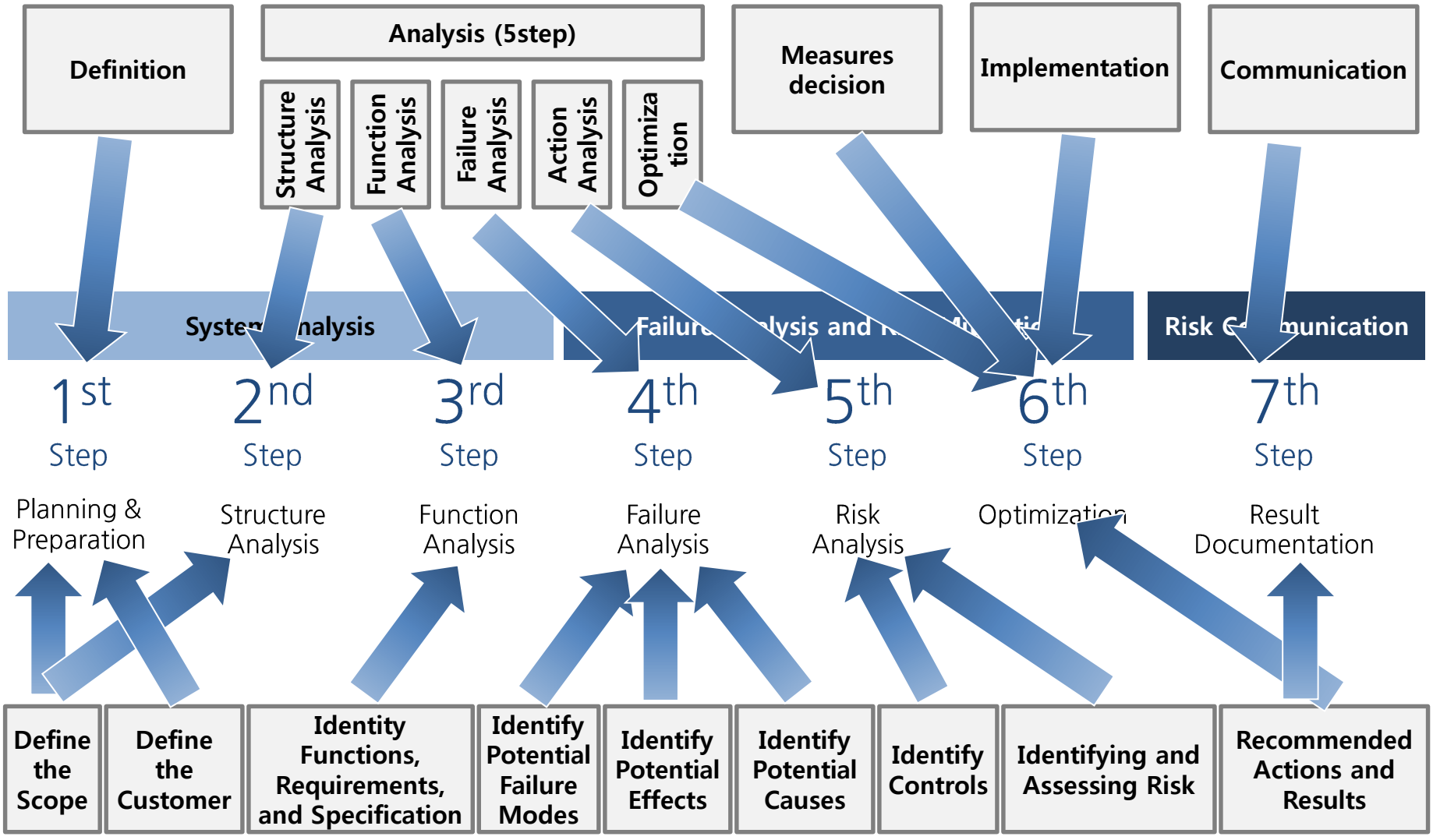
- (FMEA) Project identification
- Project plan: inTent, Timing, Team, Tasks, Tool (5T)
- Analysis boundaries : What is included and excluded from the analysis
- Identification of baseline FMEA with lessons learned
- Basis for the Structure Analysis step

❖ Increased Criteria Specificity

- More specificity in the criteria to determine levels for Severity, Occurrence, and Detection ratings.
- Action Priority (AP) replaces RPN (Risk Priority Numbers).

1. AIAG-VDA FMEA Handbook 소개

❖ 기존 VDA, AIAG FMEA 대비 차이점 : 큰 틀에서 보면 완전히 새로운 것은 아님.



1. AIAG-VDA FMEA Handbook 소개

System Analysis		
Planning & Preparation	**Structure Analysis**	**Function Analysis**
Project identification	Visualization of the analysis scope	Visualization of functions
Project plan: inTent, Timing, Team, Task, Tool (5T)	Structure tree of equivalent: block diagram, boundary diagram, digital model, physical parts	Function tree/net or function analysis form sheet and parameter diagram
Analysis boundaries: What is included and excluded from the analysis	Identification of design interfaces, interactions, close clearances	Association of requirements or characteristics to functions. Cascade of customer (external and internal) functions with associated requirements
Identification of baseline FMEA with lessons learned	Collaboration between customer and supplier engineering team (interface responsibilities)	Collaboration between engineering teams (systems, safety, and components)
Basis for the Structure Analysis step	Basis of the Function Analysis	Basis of the Failure Analysis step

1. AIAG-VDA FMEA Handbook 소개

Failure Analysis and Risk Mitigation			Risk Communication
Failure Analysis	**Risk Analysis**	**Optimization**	**Results Documentation**
Establishment of the Failure chain	Assignment of **existing and/or planned** controls and rating of failure	Identification of the actions necessary to reduce risks	Communication of results and conclusions of the analysis
DFMEA Potential Failure Effects, Failure Modes, Failure Causes for each product function. **FMEA-MSR** Potential Failure Cause, Monitoring, System Response, Reduced Failure Effect	**DFMEA** Assignment of Prevention Controls to the Failure Causes Assignment of Detection Controls to the Failure Causes and/or Failure Modes **FMEA-MSR** Assignment of a Rationale for Frequency Rating Assignment of Monitoring Controls Analysis of Provisions for functional safety and regulatory compliance	Assignment of responsibilities and deadlines for action implementation	Establishment of content of the documentation
Identification of product failure causes using a parameter diagram or failure network	**DFMEA** Rating of Severity, Occurrence and Detection for each failure chain Evaluation of Action Priority **FMEA-MSR** Rating of Severity, Frequency and Monitoring for each failure chain Evaluation of Action Priority	Implementation of actions taken including confirmation of the effectiveness of the implemented actions and assessment of risk after actions taken	Documentation of actions taken including confirmation of the effectiveness of the implemented actions and assessment of risk after actions taken
Collaboration between customer and supplier (Failure Effects)	Collaboration between customer and supplier (Severity)	Collaboration between the FMEA team, management, customers, and suppliers regarding potential failures	Communication of actions to reduce risks, including within the organization, and with customers and/or supplier as appropriate
Basis for the documentation of failures in the FMEA form and the Risk Analysis step	Basis for the product or process Optimization step	Basis for refinement of the product requirements and prevention and detection controls	Record of risk analysis and reduction to acceptable levels.

1. AIAG-VDA FMEA Handbook 소개

❖ Product General Evaluation Criteria Severity (S)

Product General Evaluation Criteria Severity (S)		
Potential Failure Effects rated according to the criteria below		
S	**Effect**	**Severity criteria**
10	**Very High**	Affects safe operation of the vehicle and/or other vehicles, the health of driver or passenger(s) or road users or pedestrians.
9		Noncompliance with regulations.
8	**High**	**Loss of primary vehicle function necessary for normal driving during expected service life.**
7		**Degradation of primary vehicle function necessary for normal driving during expected service life.**

- **Warning의 유무와 관계 없이 신체 상해에 관련된 Effect는 S10 (Safety is 10 regardless of warning, and 9 is regulatory).**

1. AIAG-VDA FMEA Handbook 소개

❖ Occurrence Rating

- O describes the occurrence potential of the failure cause during the **lifecycle of the vehicle**, taking into account the associated preventive action.
- In the preventive preparation of the FMEA, O-value expected according to the current state of knowledge is assessed **before the execution of the detection actions.**
- After the application of the detection action during development and verification of the effectiveness of the preventive actions, the **O-evaluation is either confirmed or corrected according to the result of the detection action.**

- The Occurrence is the likelihood that a specific cause/mechanism will occur resulting in the failure mode **within design life.**

- The Occurrence rating describes the potential of the failure cause to **occur in customer operation**, according to the rating table, **considering results of already completed detection controls.**

1. AIAG-VDA FMEA Handbook 소개

❖ Occurrence DFMEA

Occurrence Potential (o) for the Product				
Potential Failure Causes rated according to the criteria below. Consider Product Experience and Prevention Controls when determining the best Occurrence estimate (Qualitative rating)				
O	**Prediction of Failure Cause Occurring**	**Occurrence criteria – DFMEA**	**Incidents per 1000 items/vehicles**	**Time Based Failure Cause Prediction**
10	**Extremely high**	**First application of new technology** anywhere without operating experience and/or under uncontrolled operating conditions. No Product verification and/or validation experience. Standards do not exist and best practices have not yet been determined. Prevention controls not able to predict field performance or do not exist.	=>100 per thousand, >/= 1 in 10	Every time
9	**Very high**	**First use of design** with technical innovations or materials within the company. New application or change in duty cycle/ operating conditions. No product verification and/or validation experience. Prevention controls not targeted to identify performance to specific requirements.	50 per thousand, 1 in 20	Almost every time
8		**First use of design** with technical innovations or materials on a new application. New application or change in duty cycle/ operating conditions. No product verification and/or validation experience. Few existing standards and best practices, not directly applicable for this design. Prevention controls not a reliable indicator of field performance.	20 per thousand, 1 in 50	More than once per shift

- **Note: O 10, 9, 8, 7 can drop based on product validation activities.**

1. AIAG-VDA FMEA Handbook 소개

❖ Detection DFMEA

Detection Potential (D) for the Validation of the Product Design			
Detection Controls rated according to Detection Method Maturity and Opportunity for Detection.			
D	**Ability to Detect**	**Detection Method Maturity**	**Opportunity for Detection**
10	**Very low**	Test procedure yet to be developed.	Test method not defined
9		Test method not designed specifically to detect failure mode or cause.	Pass-Fail, Test-to-Fail, Degradation Testing
8	**Low**	New test method; not proven.	Pass-Fail, Test-to-Fail, Degradation Testing
7		Proven test method for verification of functionality or validation of performance, quality, reliability and durability; planned timing is later in the product development cycle such that test failure may result in production delays for re-design and/or re-tooling	Pass-Fail testing
6	**Moderate**		Test-to-Failure
5			Degradation Testing

1. AIAG-VDA FMEA Handbook 소개

❖ Action Priority DFMEA - High, Medium, Low

Priority High (H): Highest priority for review and action. The team **needs** to either identify an appropriate action to improve Prevention and/or Detection Controls or justify and document why current controls are adequate.

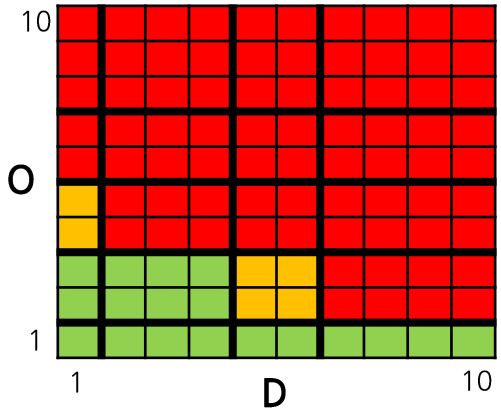
Priority Medium (M): Medium priority for review and action. The team **should** identify appropriate actions to improve prevention and/or detection controls or discretion of the company, justify and document why current controls are adequate.

Priority Low (L): Low priority for review and action. The team **could** identify actions to improve prevention and/or detection controls.

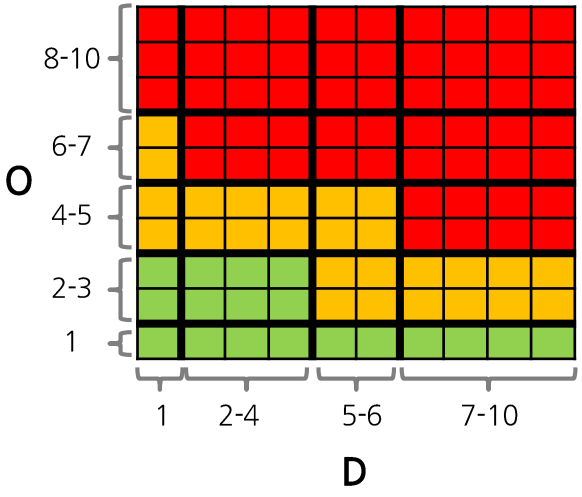
1. AIAG-VDA FMEA Handbook 소개

❖ Action Priority DFMEA & PFMEA - High, Medium, Low

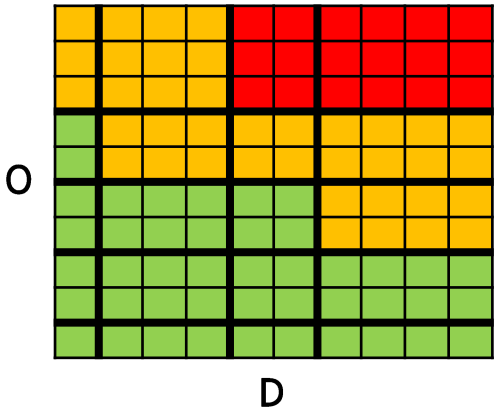
S 9-10



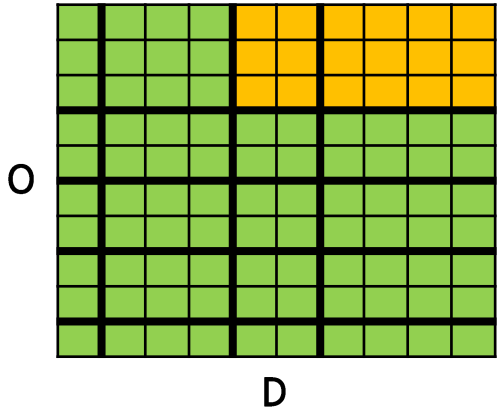
S 7-8



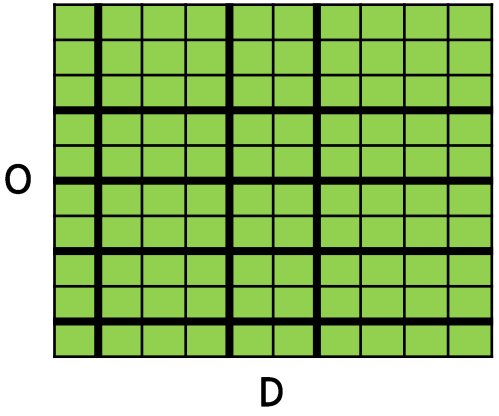
S 4-6



S 2-3



S 1



2. 새로운 분석 접근법의 적용

❖ Draft version의 적용 후 Feedback - VDA

<FMEA Alignment VDA and AIAG - VDA QMC /February 2018>

	DFMEA				PFMEA				D&PFMEA			
Question	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Introduction	0	0	0	10	0	0	0	12	0	0	0	22
Basis of FMEA	0	0	0	10	0	0	0	12	0	0	0	22
External and Internal Req.	0	0	0	10	0	0	2	10	0	0	2	20
Demand for Action & Timing	0	0	0	10	0	0	3	9	0	0	3	19
Definition and Description	0	0	0	10	0	0	1	11	0	0	1	21
1st Step: Scope definition	0	0	2	8	0	0	2	10	0	0	4	18
2nd Step: Structure analysis	0	0	2	8	0	0	1	11	0	0	3	19
3rd Step: Function analysis	0	0	4	6	0	0	3	9	0	0	7	15
4th Step: Failure analysis	0	0	0	10	0	0	0	12	0	0	0	22
5th Step: Risk analysis	0	0	2	8	0	0	5	7	0	0	7	15
6th Step: Optimization	0	0	1	9	0	0	2	10	0	0	3	19
Annex	0	0	1	9	0	0	5	7	0	0	6	16
Rating chart: Severity	0	0	1	9	0	0	2	10	0	0	6	16
Rating chart: Occurrence	0	0	1	9	0	0	5	7	0	0	3	19
Rating chart: Detection	0	0	0	10	0	1	3	7	0	1	3	17
FMEA Spreadsheet & Rep	0	0	1	9	0	0	3	8	0	0	4	17
Percentage	**0%**	**0%**	**9%**	**91%**	**0%**	**0%**	**19%**	**80%**	**0%**	**0%**	**15%**	**85%**

Question 1	I don't get it
Question 2	I understand partially, but would need some help in application
Question 3	I understand the major concepts, but have some questions on the details
Question 4	I get it, it is clear

2. 새로운 분석 접근법의 적용

❖ Draft version의 적용 후 Feedback - AIAG

<FMEA Alignment VDA and AIAG - VDA QMC /February 2018>

	DFMEA				PFMEA				D&PFMEA			
Question	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Introduction	0	0	0	11	0	0	2	16	0	0	2	27
Basis of FMEA	0	0	0	11	0	0	1	17	0	0	1	28
External and Internal Req.	0	1	2	7	0	0	3	15	0	1	5	22
Demand for Action & Timing	0	0	2	10	0	0	2	15	0	0	4	25
Definition and Description	0	0	3	8	0	0	3	15	0	0	6	23
1st Step: Scope definition	0	0	4	7	0	0	5	13	0	0	9	20
2nd Step: Structure analysis	0	3	6	2	0	1	7	10	0	4	13	12
3rd Step: Function analysis	0	5	5	1	0	7	8	3	0	12	13	4
4th Step: Failure analysis	0	2	8	1	0	1	6	10	0	3	14	11
5th Step: Risk analysis	0	1	5	4	0	1	3	13	0	2	8	17
6th Step: Optimization	0	1	5	4	0	1	1	15	0	2	6	19
Annex	0	0	1	3	1	1	2	11	1	1	3	14
Rating chart: Severity	0	1	3	6	0	0	7	10	0	1	10	16
Rating chart: Occurrence	0	1	3	6	0	0	8	9	0	1	11	15
Rating chart: Detection	0	1	3	6	0	0	4	13	0	1	7	19
FMEA Spreadsheet & Rep	0	2	3	1	0	1	4	9	0	3	7	10
Percentage	**0%**	**11%**	**32%**	**58%**	**0%**	**4%**	**24%**	**72%**	**0%**	**7%**	**27%**	**66%**

Question 1	I don't get it
Question 2	I understand partially, but would need some help in application
Question 3	I understand the major concepts, but have some questions on the details
Question 4	I get it, it is clear

2. 새로운 분석 접근법의 적용

❖ Draft version의 적용 후 Feedback - VDA&AIAG

<FMEA Alignment VDA and AIAG - VDA QMC /February 2018>

	VDA-DFMEA				AIAG-DFMEA			
Question	1	2	3	4	1	2	3	4
1st Step: Scope definition	0	0	2	8	0	0	4	7
2nd Step: Structure analysis	0	0	2	8	0	3	6	2
3rd Step: Function analysis	0	0	4	6	0	**5**	5	1
4th Step: Failure analysis	0	0	0	10	0	2	8	1
5th Step: Risk analysis	0	0	2	8	0	1	5	4
6th Step: Optimization	0	0	1	9	0	1	5	4

Question 1	I don't get it
Question 2	I understand partially, but would need some help in application
Question 3	I understand the major concepts, but have some questions on the details
Question 4	I get it, it is clear

- **VDA 기반의 FMEA를 수행하던 조직은 변경에 대한 대응에 특별한 어려움이 없을 것으로 판단됨**
- **AIAG 기반의 FMEA를 수행하던 조직은 구조분석→ 기능분석 → 고장 분석으로 이어지는 새로운 방법론에 대한 학습/연습 필요**

2. 새로운 분석 접근법의 적용

❖ New DFMEA Standard Template 이용

Design Failure Mode and Effect Analysis (DESIGN FMEA)

PLANNING & PREPARATION (STEP 1)

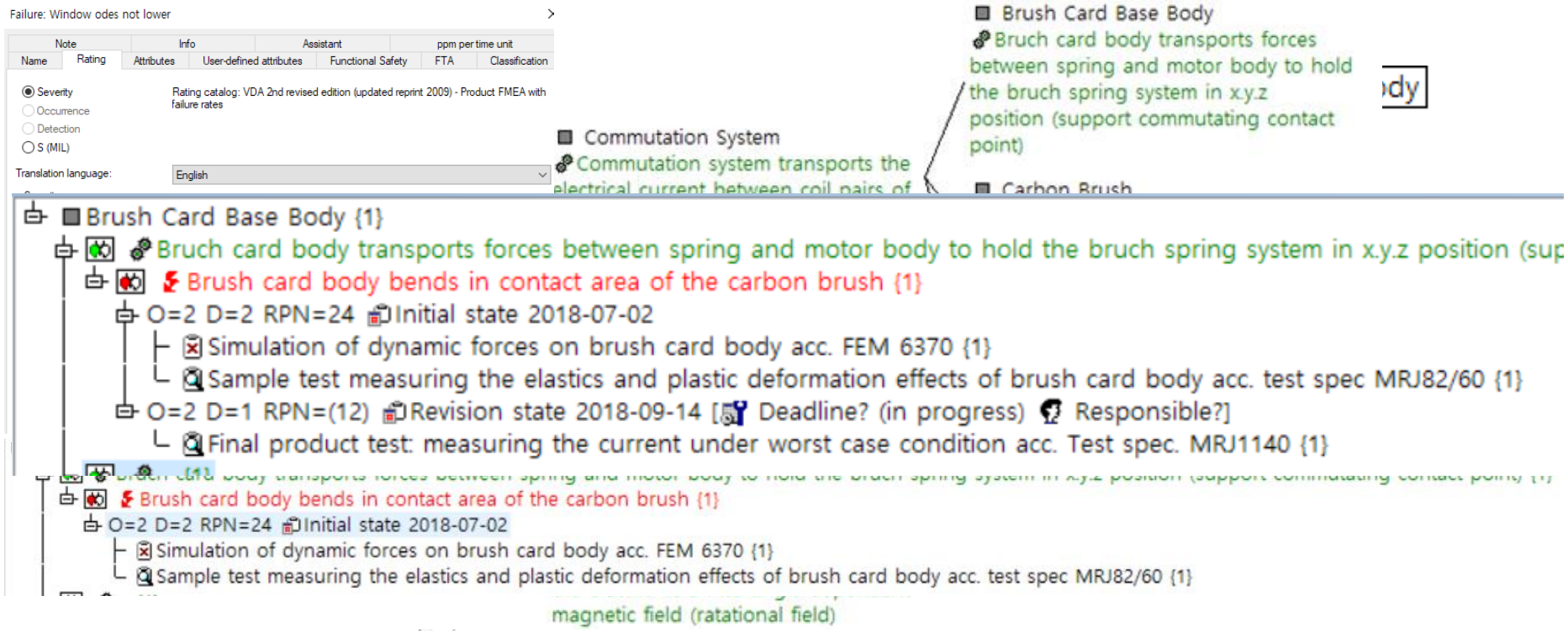
Company Name:	Acme Automotive	Subject:	PX123 Upper Jacket	DFMEA ID Number:	12345
Engineering Location:	Munich, Germany	DFMEA Start Date:	19-Mar-2018	Design Responsibility:	S, Gray
Customer Name:	Jackson Industry	DFMEA Revision Date:	25-Sep-2018	Confidentiality Level:	Confidential
Model/ Year/ Platform:	2020 PX123	Cross Functional Team:	See Team List		

	CONTINUOUS IMPROVEMENT	STRUCTURE ANALYSIS (STEP 2)			FUNCTION ANALYSIS (STEP 3)			FAILURE ANALYSIS (STEP 4)			
Issue #	History/ Change Authorization (As Applicable) (This column is optional)	1. Next Higher Level	2. Focus Element	3. Next Lower Level or Characteristic Type	1. Next Higher Level Function and Requirement	2. Focus Element Function and Requirement	3. Next Lower Level Function and Requirement or Characteristic	1. Failure Effect (FE) to the Next Higher Level Element and/or Vehicle End User	Severity (S) of FE	2. Failure Mode (FM) of Focus Element	3. Failure Cause (FC) of the Next Lower Level or Characteristic
		Window Lifter Motor	Commutation System	Brush Card Base Body	Convert electrical energy into mechanical energy according to parameterization	Communication system transports the electrical current between coil pairs of the electromagnetic converter	Brush card body transports forces between spring and motor body to hold the brush spring system in x, y, z position (support commutating contact point)	Torque and rotating velocity of the window lifter motor too low	6	Angle deviation by commutation system intermittently connects the wrong coils (L1, L3 and L2 instead of L1, L2 and L3)	Brush card body bends in contact area of the carbon brush

RISK ANALYSIS (STEP 5)						OPTIMIZATION (STPE 6)											
Current Prevention Control (PC) of FC	Occurrence (O) of FC	Current Detection Controls (DC) of FC or FM	Detection (D) of FC/FM	DFMEA AP	Filter Code (Optional)	DFMEA Preventive Action	DFMEA Detection Action	Responsible Person's Name	Target Completion Date	Status	Action Taken with Pointer to Evidence	Completion Date	Severity (S)	Occurrence (O)	Detection (D)	DFMEA AP	Filter Code (Optional)	Remarks
Simulation of dynamic forces on brush card body acc. FEM 6370	2	Sample test: measuring the elastics and plastic deformation effects on brush card body acc. test spec MRJ82/60	2	L		None	Final product test: measuring the current under worst case conditions acc. Test spec MRJ1140	Test Engineer Mr. Max Mueller	dd.mm.yyyy	planned			6	2	1	L		

2. 새로운 분석 접근법의 적용

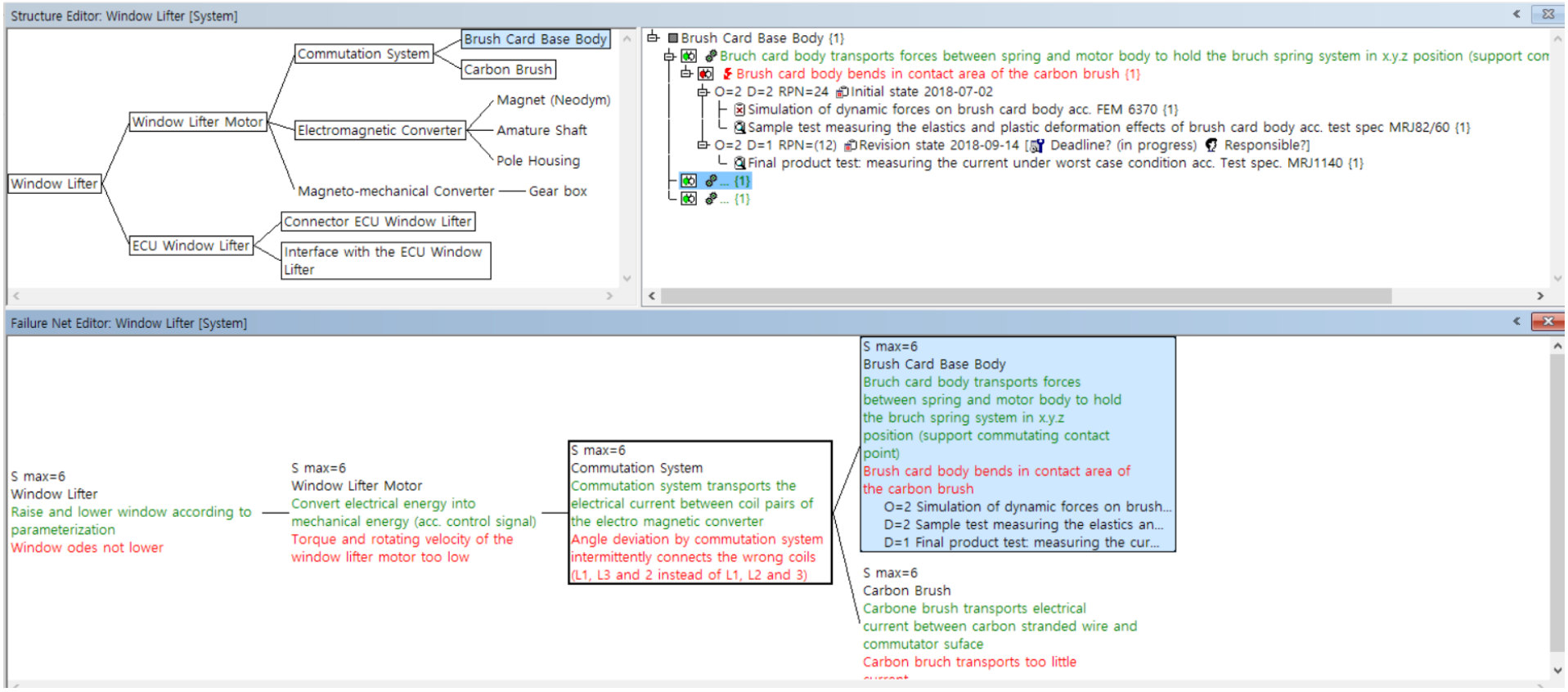
❖ 전용 도구의 이용



2nd Step

2. 새로운 분석 접근법의 적용

❖ 전용 도구의 이용



- FMEA 수행 접근법을 그대로 반영하여 구현된 도구 사용을 통해 보다 효과적인 FMEA수행 가능

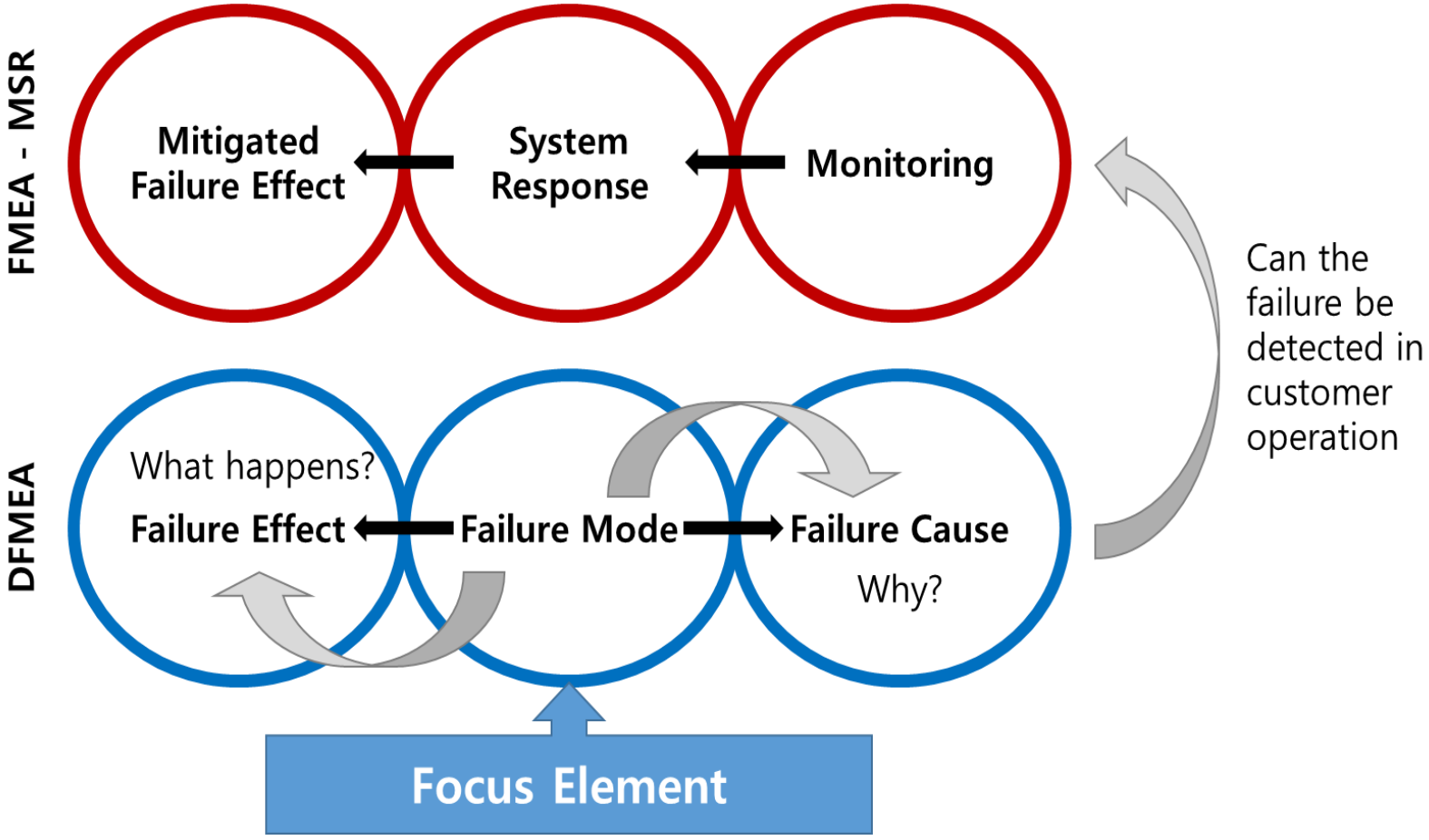
3. FMEA-MSR

❖ Supplemental FMEA for Monitoring and System Response 주요 개념

- 발생한 고장 원인 또는 고장 모드가 Customer Operation동안 운전자 또는 시스템에 의해 감지되는가?
- Customer Operation = End-user operation + in-service operation + maintenance operation
- F (frequency)는 고려되는 Customer Operational Condition과 고장이 발생할 가능성
- M (monitoring)은 고장 모드 또는 고장 원인의 감지 및 시스템 반응의 적절성 및 적시성
- DFMEA에서의 감지는 보완적인 FMEA-MSR에서의 모니터링과 다르다. Detection controls는 개발 및 validation에서 요구사항의 충족을 입증하기 위한 테스팅의 능력을 문서화한다. 이미 시스템 설계의 일부인 모니터링의 경우, validation은 모니터링과 시스템 반응이 의도한대로 동작하는지를 입증하기위한 것이다. 반대로 FMEA-MSR의 모니터링은 사양이 충족되었다는 가정하에, 고객 운용에서 결함 감지 성능의 효과성을 평가한다. 모니터링 등급은 모니터링된 결함에 대한 시스템 반응의 안전 성능 및 신뢰성을 포함한다. 이것은 안전 목표 달성의 평가에 기여하고 안전 컨셉을 도출하는데 사용될 수도 있다.
- VDA FMEA Annex A2.1의 FMEA for Mechatronical Systems을 보다 구체화 함

3. FMEA-MSR

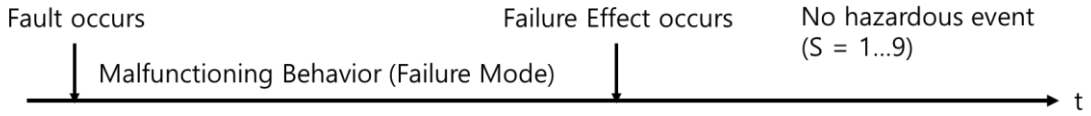
❖ Supplemental FMEA for Monitoring and System Response, 접근 방법



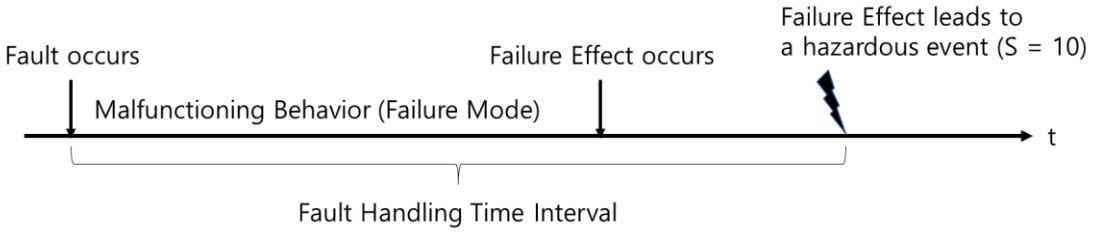
3. FMEA-MSR

❖ Severity 10, 1~9의 구분 및 Monitoring수단의 적용 유무에 따른 결과(Effect)의 차이

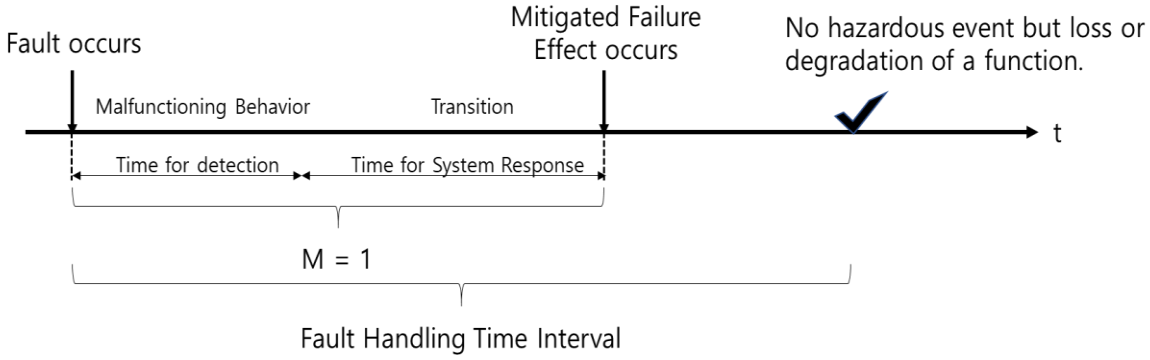
①



②

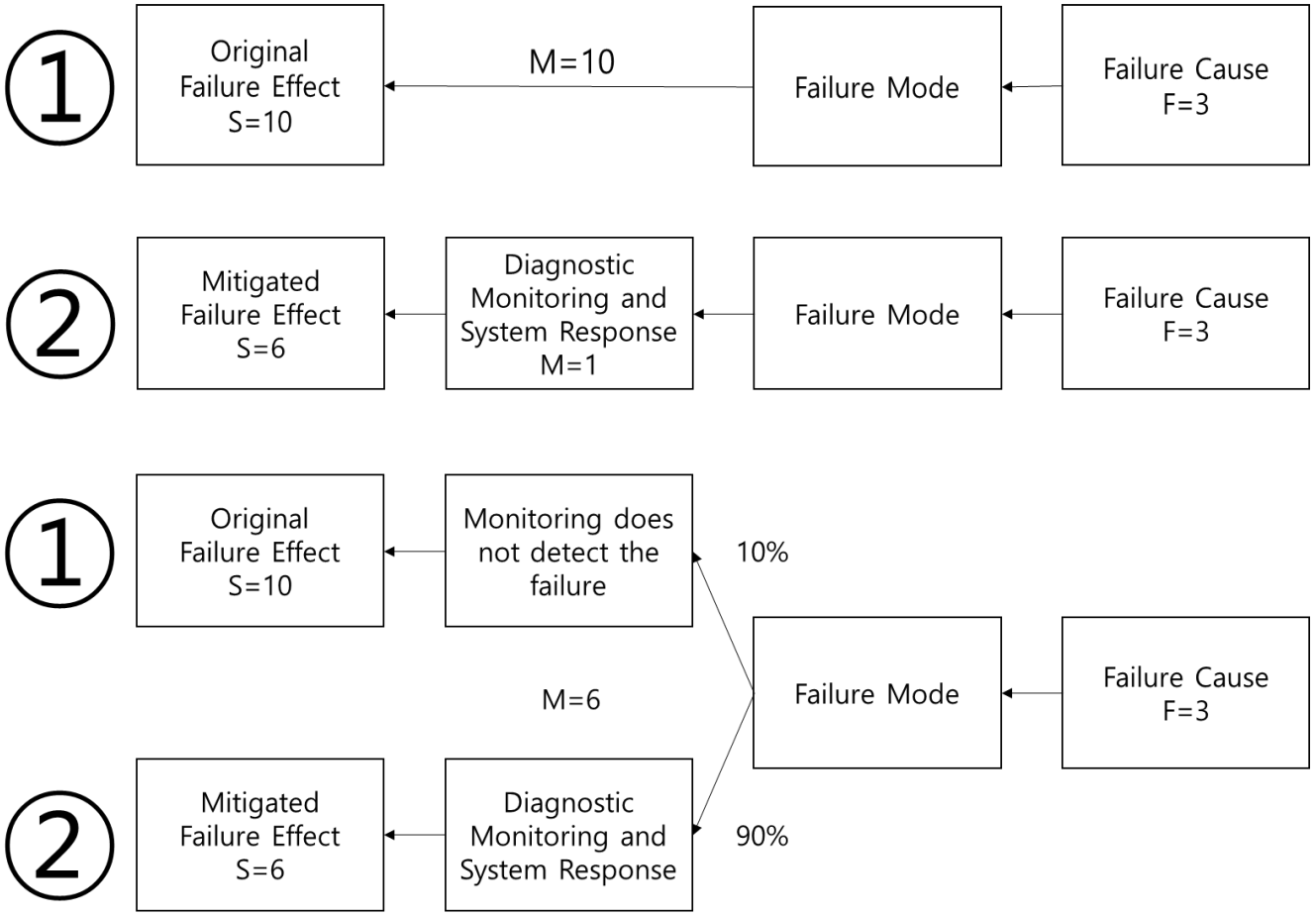


③



3. FMEA-MSR

❖ Monitoring이 M=1으로 평가되는 경우에만 Severity를 완화된 새로운 Effect에 대한 Severity로 교체 가능



❖ Frequency

D2.2 Linkage between Frequency (F) and Exposure in ISO 26262

Exposure in ISO 26262 refers to the duration or frequency of an operational situation. However, Frequency in FMEA-MSR refers to the occurrence of a fault during an operational situation. Therefore, **the two metrics are related, but not equivalent.**

Percentage of relevant operating condition in comparison to overall operating time	Value by which F may be lowered
<10%	1
<1%	2

D2.3 Linkage between Frequency (F) and FIT Rates in ISO 26262

Frequency is a qualitative estimation of how often the considered failure cause may occur during an operational situation. **FIT Rate are a quantitative assessment** of the measured reliability of an E/E component, base on exposure of the component to specific test conditions. Therefore, **the two metrics are related, but not equivalent.**

❖ Monitoring

D2.4 Linkage between Monitoring (M) and Diagnostic Coverage in ISO 26262

Monitoring (M) considers the ability of persons and/or the system to detect a specific cause (fault or failure), and react to that detected fault or failure within the Fault Tolerant Time Interval (FTTI). Diagnostic Coverage in ISO 26262 refers to the ability of the system to detect a percentage of all possible faults, and react to a fault within the Fault Tolerant Time Interval (FTTI). Therefore, the Monitoring rating in FMEA-MSR has a wider scope of detection, but **relates only to a specific cause.**

❖ Risk - ISO 26262-2018

combination of the probability of occurrence of harm and the severity of that harm

$$R = F(\textit{occurrence of harm, the severity of that harm})$$

$$R = F(f, C, S)$$

[R risk, f frequency of occurrence, C controllability, S severity]

$f = E \times \lambda$ [E exposure, λ failure rate]

3. FMEA-MSR

❖ FMEA-MSR의 Frequency 평가 기준

Frequency Potential (F) for the Product			
Frequency criteria (F) for the estimated occurrence of the Failure Cause in relevant operating situations during the intended service life of the vehicle			Blank until filled by user
F	Estimated Frequency	Frequency criteria - FMEA-MSR	Corporate or Product Line Examples
4	Low	Failure Cause is predicted to occur rarely in the field during the intended service life of the vehicle. **At least ten occurrences in the field are predicted.**	
3	Very low	Failure Cause is predicted to occur in isolated cases in the field during the intended service life of the vehicle. **At least one occurrence in the field is predicted.**	
2	Extremely low	Failure Cause is predicted not to occur in the field during the intended service life of the vehicle based on prevention and detection controls and field experience with similar parts. Isolated cases cannot be ruled out. **No proof it will not happen.**	
1	Cannot Occur	Failure Cause cannot occur during the intended service life of the vehicle or is virtually eliminated. **Evidence that Failure Cause cannot occur. Rationale is documented.**	

Percentage of relevant operating condition in comparison to overall operating time	Value by which F may be lowered
<10%	1
<1%	2

NOTE: Probability increases as number of vehicle are increased
Reference value for estimation is one million vehicle in the field.

3. FMEA-MSR

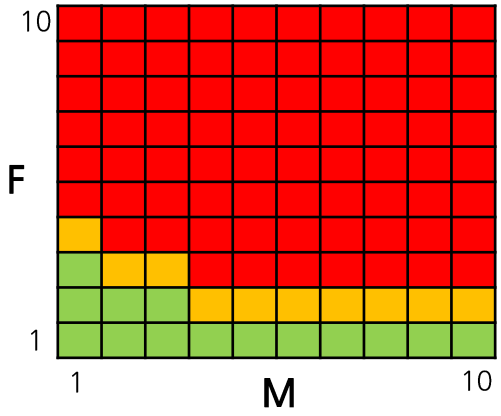
❖ FMEA-MSR의 Monitoring 평가 기준

Supplemental FMEA for Monitoring and System Response (M)			
Monitoring Criteria (M) for Failure Causes, Failure Modes and Failure Effects by Monitoring during Customer Operation. Use the rating number that corresponds with the least effective of either criteria for Monitoring or System Response			
M	Effectiveness of Monitoring Controls and System Response	Diagnostic Monitoring /Sensory Perception Criteria	System Response/ Human Reaction Criteria
4	Moderately High	The fault/failure will be automatically detected by the system during the Fault Handling Time Interval, with medium variance in detection time, or detected by the driver in most operating conditions. **Diagnostic coverage estimated >97%.**	The automated system or the driver will be able to react to the detected fault/failure during the Fault Handling Time Interval, in most operating conditions.
3	High	The fault/failure will be automatically detected by the system during the Fault Handling Time Interval with very low variance in detection time, and with a high probability. **Diagnostic Coverage estimated >99%**	The system will automatically react to the detected fault/failure during the Fault Handling Time Interval in most operating conditions with very low variance in system response time, and with a high probability.
2	Very High	The fault/failure will be detected automatically by the system with very low variance in detection time during the Fault Handling Time Interval, and with a very high probability. **Diagnostic coverage estimated >99.9%.**	The system will automatically react to the detected fault/failure during the Fault Handling Time Interval with very low variance in system response time, and with a very high probability.
1	Reliable and acceptable for elimination of original Failure Effect	The fault/failure will always be detected automatically by the system. **Diagnostic coverage estimated to be significantly greater than 99.9%.**	The system will always automatically react to the detected fault/failure during the Fault Handling Time Interval.

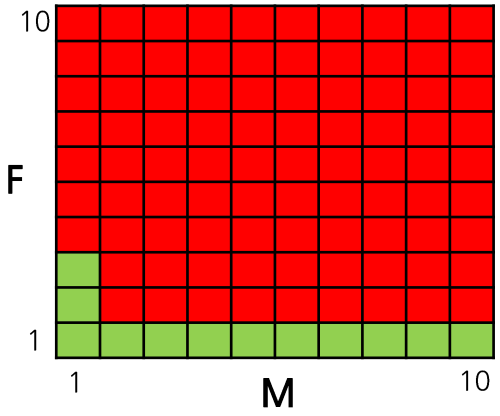
3. FMEA-MSR

❖ Action Priority FMEA-MSR - High, Medium, Low

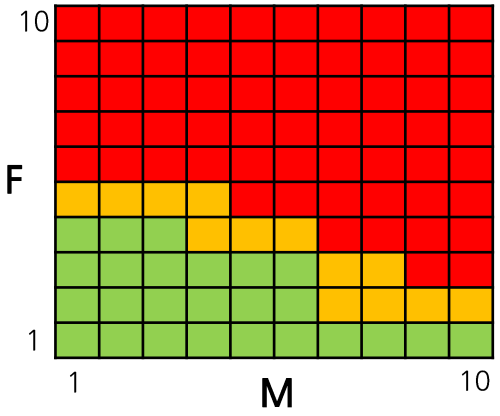
S 10



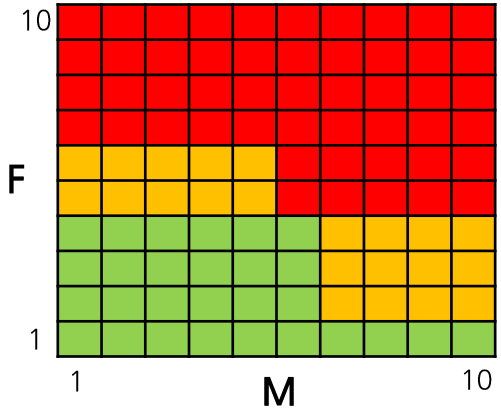
S 9



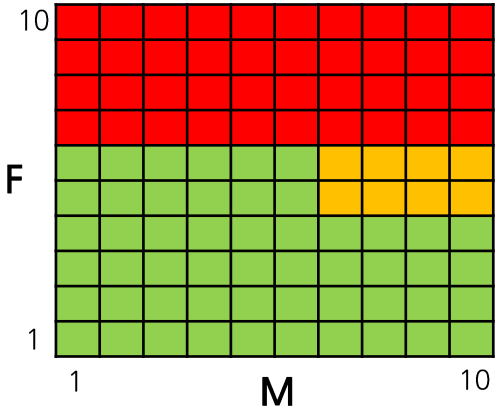
S 7-8



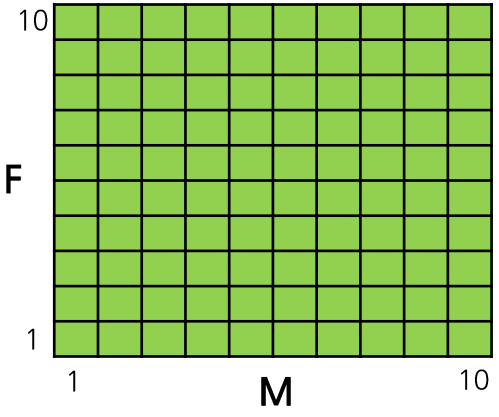
S 4-6



S 2-3



S 1

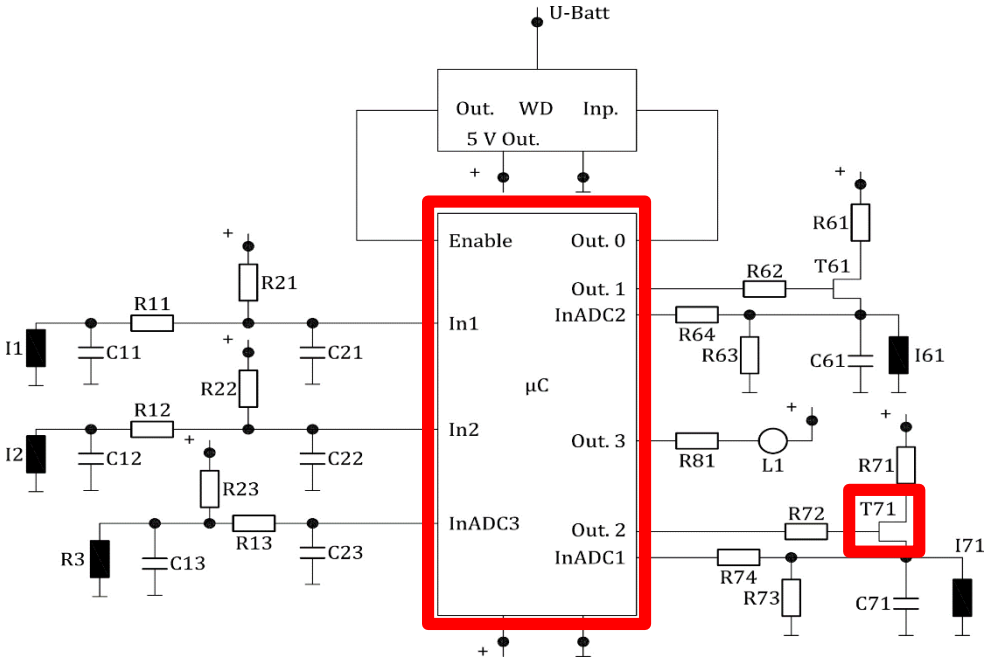


4. FMEA-MSR 적용 AP평가 예

❖ FMEA-MSR S, F, M rating 예 (ISO 26262-5:2018 Annex E)

Safety goal 1 : valve 2 shall not be closed for longer than 100 ms when the temperature is higher than 100 °C". ASIL B. (assumption E2(duration), C3, S3), safe state : valve 2 open.

➔ ASIL B assigned : S10



Component Name	FIT	Safety related	Failure mode	FM Dist.	SG violation	SM	SM Coverage
T71	5	Yes	Open	50%		SM1	
			Short	50%	X		90%
µC	100	Yes	All	50%	X	SM4	90%
			All	50%			

4. FMEA-MSR 적용 AP평가 예

❖ FMEA-MSR S, F, M rating 예 (ISO 26262-5:2018 Annex E)

Safety goal 1 : valve 2 shall not be closed for longer than 100 ms when the temperature is higher than 100 °C". ASIL B. (assumption E2(duration), C3, S3), safe state : valve 2 open.

➔ ASIL B assigned : S10

Case 1. T71's short circuit (2.5FIT) leads to violation of SG1 & 90% coverage Safety Mechanism is implemented .

- short circuit의 발생 가능성은 $2.5x10^{-9}$/h, Handbook 기준 100만(10^6)대의 차량, HARA평가에서 E2로 고려되는 전체 주행 시간 대비 1%미만임을 가정, 일반적인 차량의 운행 시간 8000시간 가정

$2.5x10^{-9} \times 8000 \times 10^6 = 20$ ➔ 10년의 보증기간동안 100만대의 차량 중 T71의 short circuit에 의한 안전목표 위반은 20회 발생 할 것으로 예측됨.

1회 예측 F3, 10회 예측 F4로 평가 기준이 마련되어 있으므로 100회 F5로 가정하면, 전체 운영 시간의 1%미만의 운용사항에서만 해당 고장 원인이 안전목표의 위반으로 이어 지므로(2단계 하향) F3로 평가.

항상 모니터링이 수행되는 90%의 Coverage를 갖는 수단이 적용, FTTI이내에 안전 상태로 천이 M5

S10, F3, M5 ➔ AP HIGH : 추가적 Monitoring 향상 또는 Frequency 감소 방안(부품변경) 필요

4. FMEA-MSR 적용 AP평가 예

❖ FMEA-MSR S, F, M rating 예 (ISO 26262-5:2018 Annex E)

Safety goal 1 : valve 2 shall not be closed for longer than 100 ms when the temperature is higher than 100 °C". ASIL B. (assumption E2(duration), C3, S3), safe state : valve 2 open.

➔ **ASIL B assigned : S10**

Case 2. microcontroller's safety related faults (50FIT) lead to violation of SG1 & 90% coverage Safety Mechanism is implemented.

- MCU의 안전 관련 결함 발생 가능성은 $50x10^{-9}$/h, Handbook 기준 100만(10^6)대의 차량, HARA평가에서 E2로 고려되는 전체 주행 시간 대비 1%미만임을 가정, 일반적인 차량의 운행 시간 8000시간 가정

$50x10^{-9} \times 8000 \times 10^6 = 400$ ➔ 10년의 보증기간동안 100만대의 차량 중 MCU의 안전 관련 결함에 의한 안전 목표 위반은 400회 발생 할 것으로 예측됨.

1회 예측 F3, 10회 예측 F4로 평가 기준이 마련되어 있으므로 100회 F5로, 1000회 가정하면, 전체 운영 시간의 1%미만의 운용사항에서만 해당 고장 원인이 안전목표의 위반으로 이어 지므로(2단계 하향) F4로 평가.

항상 모니터링이 수행되는 90%의 Coverage를 갖는 수단이 적용, FTTI이내에 안전 상태로 천이 M5

S10, F4, M5 ➔ AP HIGH : 추가적 Monitoring 향상 또는 Frequency 감소 방안(부품변경) 필요

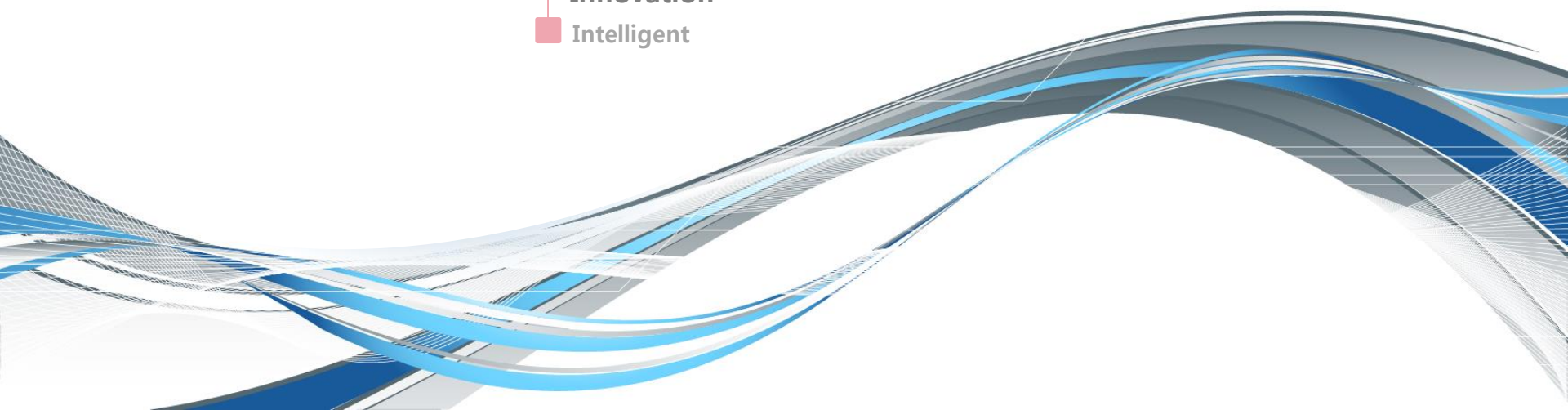
Smart
System
Software

Process
Product
Professional
People

Durable
Delivery
Deployment

SPID

Improvement
Innovation
Intelligent



㈜에스피아이디
서울시 금천구 가산동 371-50 에이스하이엔드타워3차 1803호
02-3453-5345 / Fax: 02-3453-5346 / spid@espid.com
www.espid.com