OMNEX

Integrating FMEAs, FMEDAs, and Fault Trees for Functional Safety

Chad Kymal
Omnex

Gregory Gruska
Omnex

SEPTEMBER 2021

Omnex Inc.
315 E. Eisenhower Parkway, Suite 214, Ann Arbor, MI 48108
Phone: (734) 761-4940 | Fax: (734) 761-4966 | Email: info@omnex.com

Key Words: Integration, FMEA, FMEDA, Fault Tree, Functional Safety, ISO 26262

SUMMARY AND CONCLUSIONS

The functional safety FMEA (Failure Mode Effects Analysis) will be shown to include both single and multi-point faults and incorporate safety mechanisms as preventive controls. Furthermore, by constructing this FMEA using requirements flow down from the System, Hardware and Software development, the FMEA can link with the FMEDA (Failure Mode Effects and Diagnostic Analysis) and the FTA (Fault Tree Analysis) and together they provide Single-Point and Latent Fault metrics (SPFM and LFM) including the "Probabilistic Metric for random Hardware Failures" (PMHF) metrics in a consistent manner.

FMEAs traditionally have only incorporated single-point faults. In this ground breaking presentation of this approach, the functional safety FMEA will be shown to include both single and multi-point faults and incorporate safety mechanisms as preventive controls. As the FMEA is filled out, the FMEDA will be populated, providing consistency between the FMEDA and FMEA techniques. The FMEA of the hardware is developed at the different levels, while the FMEDA is at the component level and the failure modes of the FMEDA are component failure modes. If the FMEA is completed using the AIAG-VDA FMEA handbook approach, where the higher level, focus level, and lower levels relationships are used and there is a cause and effect relationship between the failure modes at the different levels, then the FTA can also be developed from the FMEA. In this way, the FMEA, FMEDA and FTA are linked documents and the FMEDA and FTA provide the single-point fault, multi-point fault, and the "Probabilistic Metric for random Hardware Failures" (PMHF) metrics in a consistent manner.

1. SAFETY ANALYSIS IN ISO 26262 FUNCTIONAL SAFETY

ISO 26262 is an automotive functional safety standard which was first released in 2011. This standard's scope is electronics and electrical safety-related in series production road vehicles excluding mopeds. In 2018, the standard was expanded to also include motorcycles, buses and trucks.

The focus of this standard is on assuring the safety of motor vehicles features and innovations against hazards (harm to humans) caused by malfunctions. With the advent of electric and autonomous vehicles, this standard and the need for safety analysis has become that much more relevant. It is important to keep in mind that in the overall topic of Safety Analysis, multi-point FMEAs, FMEDAs, and FTAs are also relevant to other industries since today's technology is much more that include mechatronic, electronic, and sensor oriented components.

Functional Safety development starts in Part 3 of the ISO 26262 framework: the Concept Phase with an Item Definition and a hazard analysis and risk analysis (HARA). This is one part of the 12 parts which make up the complete standard as shown in Figure 1. Part 3 is the beginning to the design cycle / process which includes Part 4: Product Development at the System Level, Part 5: Product Development at the Hardware Level and Part 6: Product Development at the Software Level.

Based on the risk analysis, malfunctions which cause harm to humans (hazards) are rated with an Automotive Safety Integrity Levels (ASILs) A, B, C, or D based on the severity, exposure, and controllability of the hazard. The hazards are used to develop safety goals that can be communicated easily within the organization and drive the rest of the safety development.

The functions and requirements that are necessary to assure the safety goals are met in the design are developed and then allocated to the elements (constituent parts) of the item based on the architecture. This is called a Functional Safety Concept (FSC).

Figure 1: ISO 26262 Framework

During the product development at the systems level, the functions and requirements that are necessary to assure the FSCs are met in the design are developed and then allocated to hardware and software elements based on the architecture. These allocated requirements are referred to as the Technical Safety Concept (TSC). At the hardware and/or software levels, the detailed development and safety and verification analysis is implemented.

When the hardware and software development verification testing is complete, the activity goes back to the systems level for system integration and testing. After successful validation testing of the item, the product is formally released to serial production and a safety case is finalized.

The verification planning and implementation shall be carried out for each phase and sub-phase of the safety lifecycle. For hardware elements, this includes safety analysis. The objective of safety analyses is to ensure that the risk of a safety goal violation due to systematic faults or random hardware faults is sufficiently low.

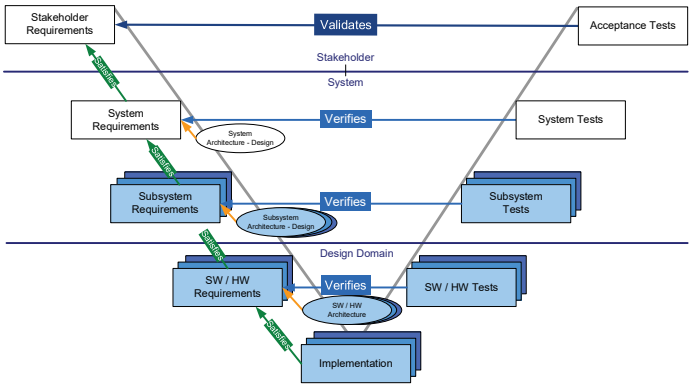

Figure 2: The V Model. This shows requirements flowing down and testing flowing up. It is important that the testing matches the level of the requirements

The scope of the safety analyses includes:

- The validation of safety goals and safety concepts
- The verification of safety concepts and safety requirements

Safety analyses are performed at the appropriate level of abstraction during the concept and product development phases. Quantitative analysis methods predict the frequency of failures while qualitative analysis methods identify failures, but do not predict the frequency of failures. Both types of analysis methods depend upon a knowledge of the relevant fault types and fault models.

By far the most popular methods for safety analysis, with the most support both in terms of standards and tools, are Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA).

As inductive and deductive methods they complement each other well.

There are industry standards (e.g., from SAE or AIAG-VDA for FMEA).

One of the latest approaches to the development of an FMEA is described in the AIAG-VDA FMEA handbook, 1st edition. The handbook provides a seven step approach, shown in Figure 3.

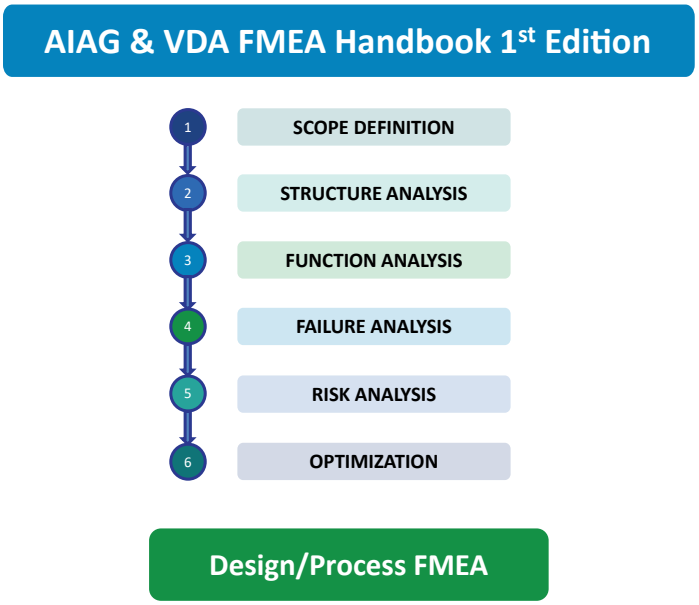

Figure 3: AIAG-VDA FMEA Seven Step Process

Step 1: Scope Definition

The main objectives of Scope Definition are:

- Definition/Selection of which aspects of the design are to be included in the analysis
- Project Plan (APQP) / Safety Plan
- Identifying relevant Lessons Learned and references
- Definition of Team Responsibilities

Step 2: Structure Analysis

Information gathered in the planning step is transferred to visualize the relationships and interactions between the design or process elements. The goal of structure analysis is to provide:

- An overview of the system structure of the product
- A definition of the system boundaries / interface description

The work products from this step are a structure tree and block diagram (preliminary architecture).

Note: the AIAG-VDA approach requires at least three levels in the structure: Higher Level > Focus Level > Lower Level (see also Figure 4).

Step 3: Function Analysis

The product or process functionality is assured by allocating purposes (function and requirements), activities or tasks intended for the product performance.

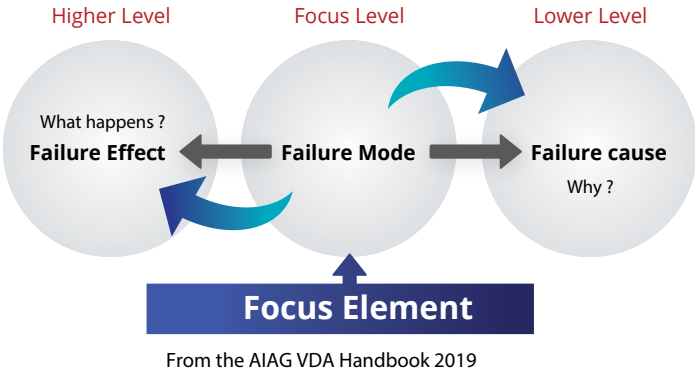

Figure 4: Focus Element

Step 4: Failure Analysis

The failures of each of the functions and requirements identified in Step 3 are identified and a Failure Net Analysis is completed, linking the effect (failure mode at the higher level) with the failure mode at the focus level with the cause (the failure mode at the lower level).

Step 5: Risk Analysis

In Step 5, the preventive and detective controls are determined together with the Action Priority (AP), which requires the identification of the severity, occurrence, and detection indices.

Step 6: Optimization

Based on the Action Priorities, preventive and/or detective improvement actions are determined. The severity, occurrence, detection, and Action Priority values are updated.

Step 7: Results Documentation

The information collected during the seven steps is used to develop the FMEA form. A management summary of the development actions and improvements is also developed.

2. LINKING FMEA, FMEDA AND FTA

All the standard approaches to FMEA used in the automotive industry to date have the same limitation: they traditionally have only incorporated single-point faults. In the past, this was not of concern since the automobile was primarily mechanical and had very few redundant (multi-point) systems. With the increased usage of electrical and electronic (E/E) items in the vehicle, especially with advanced driver-assistance systems (ADAS) and electric vehicles, this is no longer true.

ISO 26262 has defined three metrics for hardware design.

The effectiveness of the architecture to cope with hardware random failures is assessed with the two architectural metrics:

SPFM – Single-Point Fault Metric

- Quantifies the impact of the potential single-point faults (immediately dangerous) to the overall cumulative failure rate.

LPM – Latent (Multi-Point) Fault Metric

- Quantifies the impact of the potentially dangerous multi-point faults (not detected nor perceived) to the cumulative failure rate less the single point and residual faults.

These are relative metrics.

- A complementary analysis is carried out to assess the acceptability of the residual risk of safety goal violation due to random hardware errors.

Probabilistic Metric for Hardware Failures (PMHF)

- This is the safety reliability metrics, that is, the probability of violation of safety goals.

These are absolute metrics.

- Within the automotive industry, the development and use of FMEAs is well established. This is not the same for FTAs and FMEDAs. So the question asked by many engineers is why do the FTA and FMEDA?

Besides FTA being highly recommended as part of the Safety Analysis for ASIL C and D Safety Goals (ISO 26262:2018), it enables the development team to:

- Identify single- and multiple-point faults
- Calculate the PMHF (reliability) of the Safety Goal
- Analyze the interfaces and relationships to determine improvement opportunities

The FMEDA is not directly identified in the standard, although the Diagnostic Coverage Analysis, which it enables, is mentioned in Parts 5 and 10. With the FMEDA approach, the development team can:

- Calculate the SPFM (Single-Point Fault Metric) and the LFM (Latent Fault Metric) for a Safety Goal
- Analyze the interfaces and relationships to determine improvement opportunities

Use of Safety Mechanisms

The discussion on Diagnostic Coverage implies the architecture includes a safety (diagnostic) mechanism. The standard does expect the technical safety requirements to specify the necessary safety mechanisms.

The safety mechanisms are technical solutions implemented by E/E functions or elements or by other technologies to detect faults or control failures in order to achieve or maintain a safe state.

- Safety mechanisms are implemented within the item to prevent faults from leading to single-point failures or to reduce residual failures and to prevent faults from being latent.
- The safety mechanism is either able to transition to, or maintain, the item in a safe state; or able to alert the driver
- Such that the driver is expected to control the effect of the failure as defined in the functional safety concept.

To evaluate the effectiveness of the Safety Mechanisms, the standard asks for a Diagnostic Coverage Analysis (e.g., FMEDA). Diagnostic Coverage is the percentage of the failure rate of a hardware element, or percentage of the failure rate of a failure mode of a hardware element that is detected or controlled by the implemented safety mechanism.

For example, the self-monitoring of the system or elements to detect random hardware faults and, if appropriate, to detect systematic failures may detect most (e.g., 95%) but not all of the possible failure modes. This may be sufficient if the failure modes not detected are "rare" or not critical.

This requirement applies to ASILs (B), C, and D.

3 DFMEA – EXPANDED TEMPLATE (SYSTEM, SUB SYSTEM OR HARDWARE)

Current implementation of FMEAs for mechatronic and electronic designs are focused on single-point faults while that of the FMEDAs and FTAs consider both single-point ("or") and multi-point ("and") faults. Furthermore, in many "traditional" organizations, the development of the FMEA is led by engineering and the FTA is led by reliability.

The assessment and evaluation work Omnex performs for product development shows major mismatches among the three techniques due to these issues. In order to align the three methodologies, each of them needs to consider single-point, multi-point, and safety mechanisms. Furthermore, the approach should not be just for safety goals but for the entire system within the scope of the analysis.

Keep in mind, the FMEA is conducted by system, sub system, hardware, and software. The FMEDA is by each Safety Goal, and the FTA is for the entire product from system or even vehicle down to the lowest element of the BOM or structure.

To improve these mismatches, we can expand the FMEA form and process to enable:

- Flows down, functions, and requirements to the system, and then to hardware and software
- Incorporates single- and multi-point faults (see Figure 5)
- Includes Special Characteristics and ASILs designations (see Figure 5)
- Incorporates Safety Mechanisms as preventive controls (see Figure 5)
- Provides a realization of the linkages among related FMEA, FMEDA and FTA documents (see Figure 6).
- With the right dashboard, it provides a chance to see what needs to be added or changed to get the expected Hardware metrics coverage

Potential Design Failure Mode and Effects Analysis

System:					Design ☐	Process ☐	Project Name:		Satellite Design					FMEA Date (Orig.):		
Subsystem:					☒	☐	Project Number:							FMEA Date (Review):		
Component:					☐	☐	Core Team:							Document Number:		
Design Authority (DA):																
Item	Function	Req	Potential Failure Mode	Potential Effect(s) of Failure	S	C	Potential Cause(s)/ Mechanism(s) of Failure	SPF MPF (&)	Current Controls Prevent.	O	Current Controls Detec.	D	RPN	Recommended Action(s)	Responsibility & Target Completion Date	Actions Results: Actions Taken
RSU5 Satellite	Stabilize Voltage Regulator	X ± Y	Doesn't Stabilize; variation excess Y	Data Communication Error	9	YC	Trace not connected schematic;	M	Training on schematic capture	3	Automatic Schematic Checkter	3	81	Implementation of Matrix/mentor Knowledge Base, pop-up property	Knowledge base- Mike Ruggles 12-17-04, Property	Knowledge base- Mike Ruggles 12-17-04, Property boxes- Joe
					9	YC	ECAD Layout Error	M	Training	2	Layout Checker	2	36			
			Insufficient Stabilization	Data Communication Error	9	YC	Vdd (C2, C3) Capacitor Values too low	S	Circuit Monitoring in ECU	2	Bench testing, EMC testing; error	3	54	Implement Development al EMC	Developmental EMC testing	
Feed Power (pin 12) Vbp			Doesn't Feed Power	XL180 Inoperative	9	YC	Trace not connected schematic	M	Training on schematic capture	3	Automatic Schematic Checkter	3	81	Implementation of Matrix/mentor Knowledge Base, pop-up property	Knowledge base- Mike Ruggles 12-17-04, Property	Knowledge base- Mike Ruggles 12-17-04, Property boxes- Joe
					9	YC	ECAD Layout Error	M	Training	2	Layout Checker	2	36			
			Feeds too little Power	XL180 Inoperative	9	YC	Resistor (R1) Value too high	S	Spec. review Circuit	3	Bench testing	3	81	none	none	none
			Feeds too much Power		9	YC	Resistor (R1) Value too low	S	Spec. review Circuit Analysis	3	Bench testing, EMC testing	3	81	Implement Development al EMC	Developmental EMC testing	

Figure 5: Example DFMEA form with additional features highlighted

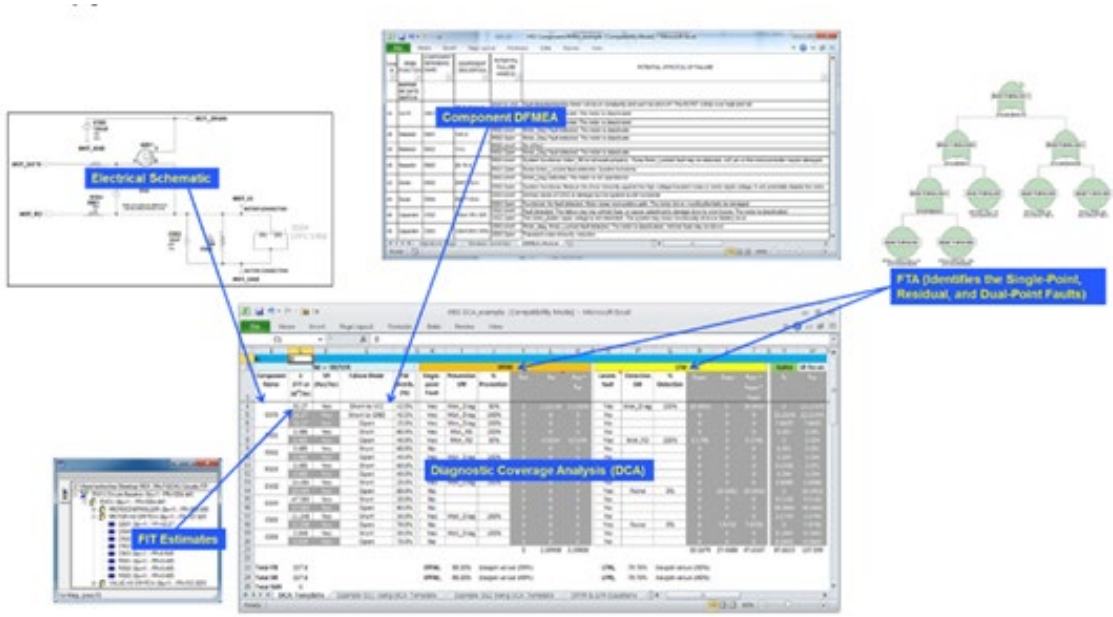

Figure 6: Interrelationships among the FMEA, FTA, and FMEDA

Much of the changes in the process are “behind the scenes” in the development software to enable the system subsystem component FMEAs interrelationship. This allows the FTA to be populated directly from the interrelated FMEAs.

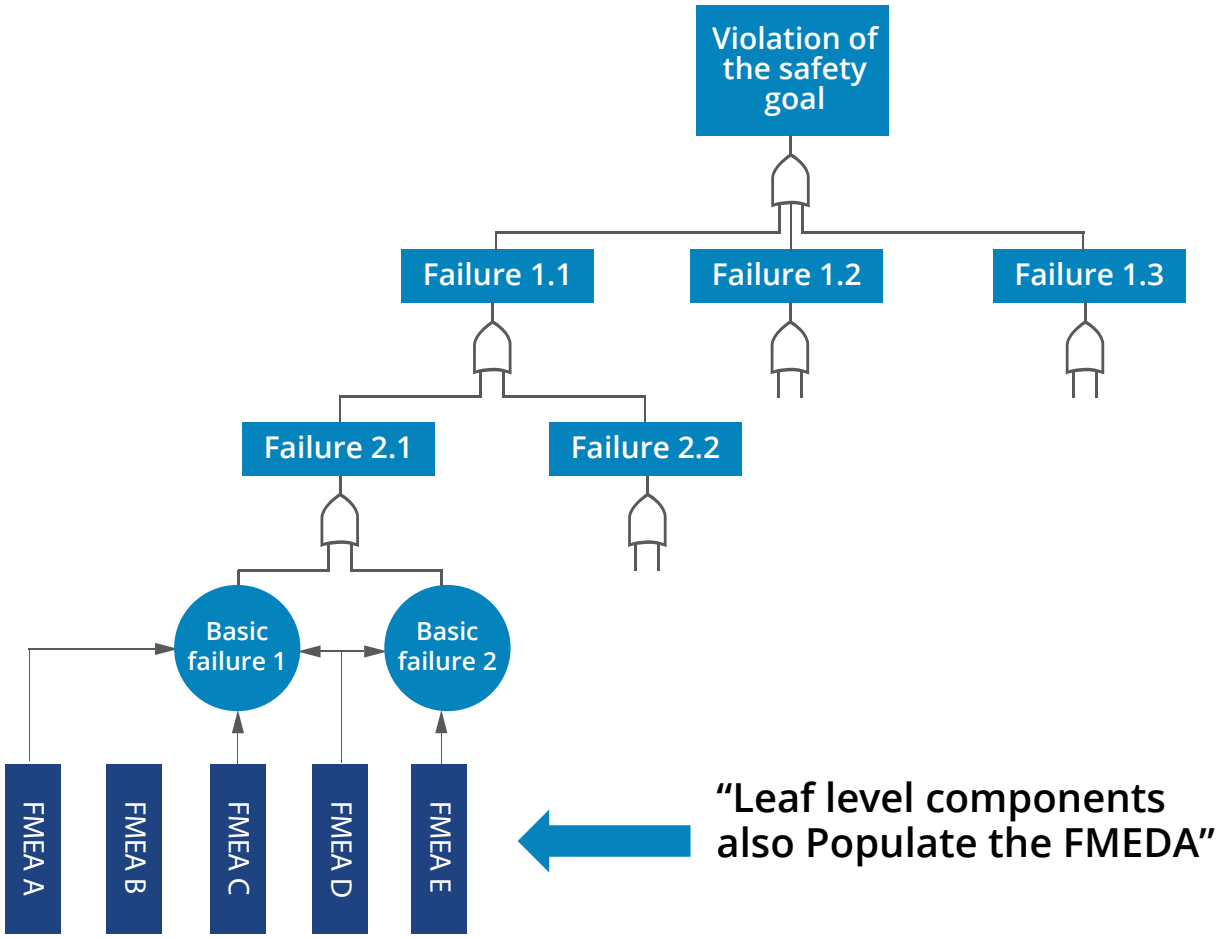

Figure 7: Flow down of FMEAs

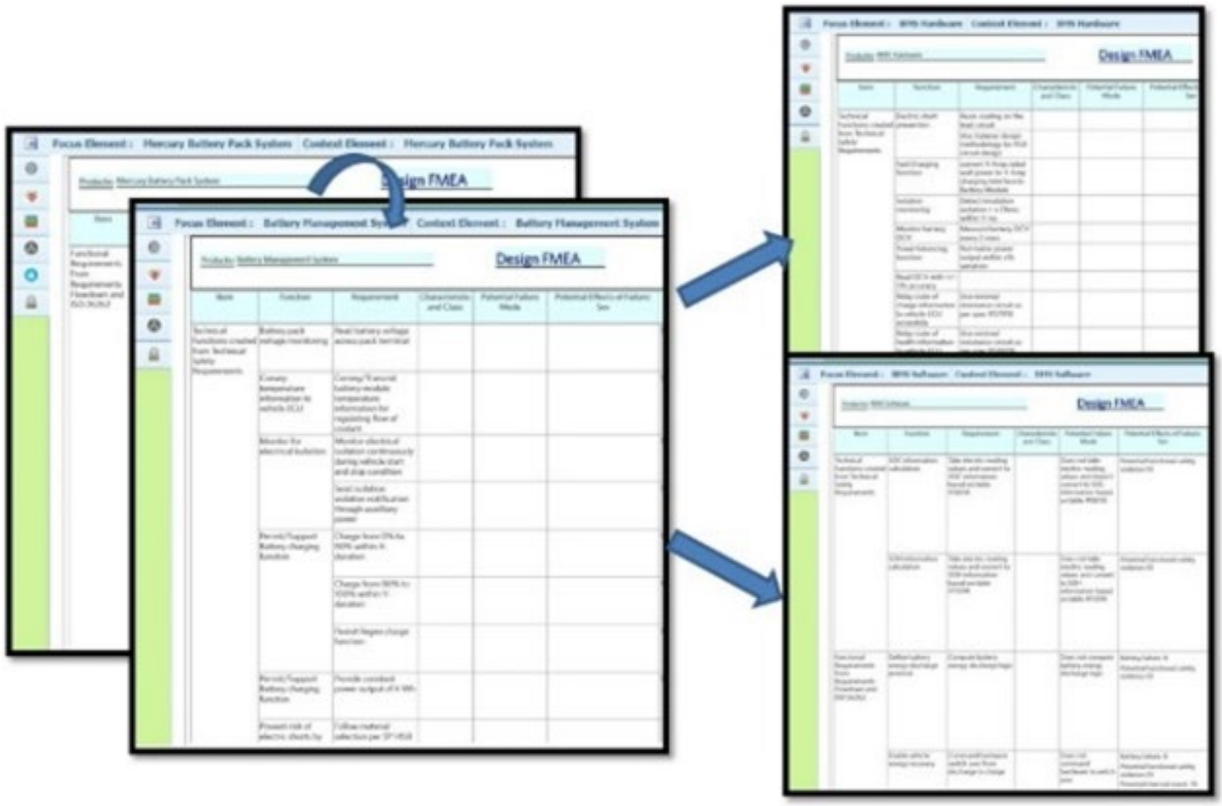

Figure 8: FTA populated from FMEA

The FTA has its focus (the top level or box) the fault related to a Safety Goal. The graphic then proceeds down through the levels of the architecture (system → subsystem → component) showing the interrelationships among the failure modes of the different levels. These failure modes can come from the expanded FMEA based on the flow down of requirements and, consequently, the causal relationship among the different levels of the design.

4. SUMMARY AND CONCLUSIONS

The system, hardware, and software FMEAs, as currently implemented, do not have functions / requirements that are currently linked or a failure flow down along the structure of the product. This linked structure allows the FMEA, FTA, and FMEDA to be linked and related to each other. Completing the FMEA completes half of the FTA or the FMEDA and vice versa. Subsequent development completing the FMEA, FTA or the FMEDA will flow to the other documents.

Omnex assessments currently shows little to no relationship between DFMEAs, FTAs and FMEDAs in most organizations. Linkages will allow for improvement in the use of the methodologies and the products in which they are used. The flow down from the safety goal to the hardware and software components with dashboards will reduce redundancy and optimize safety mechanism placement and therefore improve the overall costs and controls in a product.

Linkages between the DFMEA and design verification plan and report (DVP&R) will allow organizations to implement the V Model with greater ease. Additionally, utilizing a web-based or cloud-based solution for functional safety, FMEA, FMEDA and FTA will help development teams with the use of the tools in a distributed design environment which typically is global and includes the supply chain.

BIBLIOGRAPHY

- AIAG, VDA, AIAG & VDA FMEA Handbook, 1st Edition, June 2019, AIAG
- Ford, GM, FCA, Potential Failure Mode & Effects Analysis, 4th Edition, June 2008, AIAG
- ISO, ISO 26262:2011, Road Vehicles - Functional Safety, ISO [WITHDRAWN]
- ISO, ISO 26262:2018, Road Vehicles - Functional Safety, ISO

GLOSSARY

AIAG, Automotive Industry Action Group

ASPICE, Automotive SPICE

BOM, Bill of Materials

DFMEA, Design FMEA

FMEA, Failure Mode Effects Analysis

FMEDA, Failure Mode Effects and Diagnostic Analysis

FTA, Fault Tree Analysis

ISO, International Organization for Standardization

VDA, German Association of the Automotive Industry (Verband der Automobilindustrie)

BIOGRAPHIES

Chad Kymal
Chief Technical Officer

Omnex Engineering and Management, Inc
315 East Eisenhower Parkway, Suite 214
Ann Arbor, MI 48108 USA

e-mail: ckymal@omnex.com

Chad Kymal is the CTO of Omnex Inc., an international consulting and training organization headquartered in the United States. Over the course of Chad's successful career, he has served on the Malcolm Baldrige Board of Examiners and has received numerous quality achievement awards, including the Quality Professional of the Year award by the American Society for Quality (ASQ) Automotive Division in 2005. He is a member of Tau Beta Pi. Chad is also on the ISO/TC 176, ISO/TC 207, PC283 committees for ISO 9001:2015 (Quality Management), ISO 14001:2015 (Environmental Management) and ISO 45001 (Health and Safety Management Systems.

Chad has spent over 20 years in system, hardware and software development in various capacities. He assesses and works in automotive system, hardware and software for Agile, ASPICE, and Functional Safety ISO 26262.

Gregory Gruska
Principal Consultant and Functional Safety Champion
Omnex Engineering and Management, Inc

315 East Eisenhower Parkway, Suite 214
Ann Arbor, MI 48108 USA

e-mail: ggruska@omnex.com

Greg Gruska is the Omnex Champion for ISO 26262, and a Fellow of the American Society for Quality (ASQ). He has led multiple ISO 26262 engagements for Omnex for over a decade. He has a strong understanding and experience in systems engineering, reliability and safety analysis in both hardware and software development. In his career Greg provided quality engineering and statistical support to all GM divisional and corporate activities. Besides the application of statistics, he is active in the development of new technologies and training in these areas. Greg is considered one of the foremost authorities on automotive risk management.

Greg is a charter member of the Greater Detroit Deming Study Group and the W. E. Deming Institute. He is an ASQ certified Quality Engineer, a licensed Professional Engineer (CA - Quality) and a member of the Board of Examiners of and Judge for the MIPEx Program (1994-2020). He was on the writing committee for the FMEA 4th.

OMNEX

Global Headquaters

Omnex Inc,.

315 E. Eisenhower Parkway, Suite 214,
Ann Arbor, MI 48108.
Phone: (734) 761-4940
Email: info@omnex.com
www.omnex.com

Omnex Canada
info-ca@omnex.com

Omnex China
info-cn@omnex.com

Omnex India
info-in@omnex.com

Omnex Malaysia
info-my@omnex.com

Omnex Europe
info@omnex.eu

Omnex Mexico
info-mx@omnex.com

Omnex Middle East
info-me@omnex.com

Omnex Saudi Arabia
info-sa@omnex.com

Omnex Singapore
info-sg@omnex.com

Omnex Thailand
info-th@omnex.com