

FMEA for SysML based system descriptions

Measures to ensure and increase the quality of system components are shifting more and more into the focus of the automotive industry. One reason for this is the alarming growth in the number of recalls, which has reached a staggering magnitude in recent times. In North America, the recall rate* for the first half of 2014 climbed to about 455% compared to 142.5% in the first half of 2013. One cause for this high figure is the usage of the same system components in different series of various vehicle manufacturers. Quality problems thus are spreading and can pose a threat to the very existence of a manufacturing company.

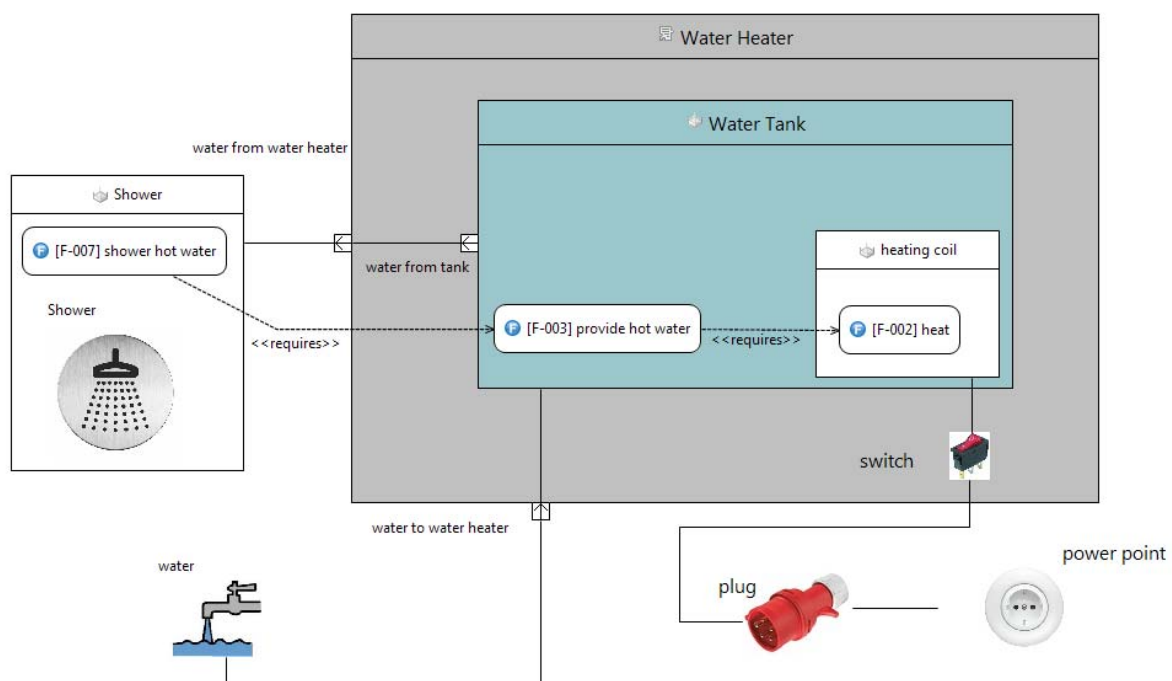
One method to prevent quality problems at an early stage is the consistent use of FMEA. It enables to identify potential failures and risks already during the system design phase and assists in defining and evaluating counter measures to control and minimize such risks. As FMEA is a well-established and widely used method, the question arises how the effectiveness and vulnerability of its use on a daily basis may have contributed to the occurrence of the described quality problems.

In practice of FMEA application often the following issues can be observed:

- The FMEA is conducted simultaneously with other development activities, however, it is not sufficiently integrated with these activities. This results in consistency problems and additional expenses/effort. In extreme cases, the FMEA does not comply with the current state of system development at all. Thus failures may not be identified or planned measures may not be sufficient.
- The measures identified in the FMEA are not adequately tracked. The measures should be incorporated in the requirement management process, which is often not possible or is left out.
- The various conducted FMEAs for parts, components, subsystems and systems are not adequately linked to each other. Hence the potential impact of failures at the component or part level on the functionality at the vehicle level is not completely visible and thus not analysed.
- Reuse is possible only to a limited extent. One should learn from mistakes - but if FMEAs are developed separately from system models, their reuse becomes difficult, i.e. failures already identified in an earlier design are simply forgotten when making new design versions or when reusing components. On the other side, referring to an FMEA of an existing previous system does not provide adequate proof of analysing the potential failures and their effects for variants or enhancements of the original system.

To overcome these problems, process modifications to tightly integrate FMEA into the development process and a consistent and rule-compliant execution of FMEA are required as well as a better linking between FMEA and underlying system models. If this is supported by an appropriate tool, the consistency problems can be quickly identified and easily resolved.

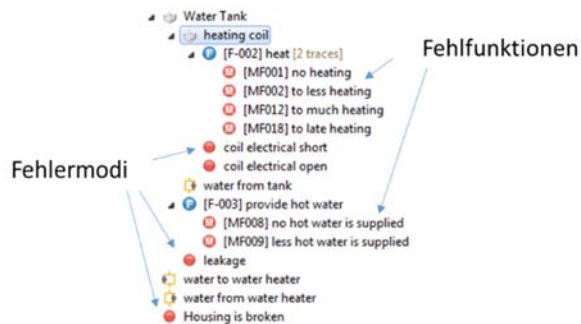
A Model-based approach using a semi-formal notation (e.g., SysML) is a key-enabler for such an improved integration of the FMEA with the activities of the system development process and to solve the consistency and efficiency problems.



Above figure gives an example for the design of a water heater using SysML. The model shows the system components as well as their hierarchy and the interconnections between them. In addition, the functions which are allocated to the individual components and the dependencies between these functions are also already defined in the model.

Thus, all essential information to initiate an FMEA is available. Moreover, in order to avoid inconsistencies and multiple work steps, even the failure modes for the components and the malfunctions for the functions can be directly added to the system model. A typical method to elicitate the malfunctions would be for example HAZOP analysis. The failure modes on the other side may be taken from the
























component/part libraries (in the case of random hardware failures) or, from statistics and surveys on the present use in the field (to cover systematic faults).



Fehlfunktionen = malfunctions

Fehlermode = failure modes

The next step is to link this information about failure modes and malfunctions using the FMEA forms. As the failure details are included as an annotation directly in the system model, this "single source of information" principle avoids for example duplications of the tree structure in different tools and the risk of inconsistencies associated with that. An FMEA form based on the SysML model is always prepopulated - the system structure including the failure modes and malfunctions is directly taken from the model. Using the forms the failure chains are identified by considering causes/effects of each individual failure mode and malfunction. Moreover, the risk assessments are carried out and the necessary measures are derived and specified also using the forms.

Component	Potential Failures	Potential Failure Effects	Severity	Max	Risk	Potential Failure Causes	Occur	Current Design Controls Prevention	Current Design Controls Detection	Detectio	RPN
 Water Heater	 Housing is broken	 [water heater hazards] flooding	0	N	 [produce housing] [MF019] mechanically broken housing is being produced	0	 [2] periodic callibration of production equipment for tank	 electrical test - coil [det: 0]	0	0	
		 [water heater hazards] electric shock	0	N	 [malfunctions at system level] [3] human misuse	0					
	 water to water heater										
	 water from water heater										
 switch	 switch electrical short	 [[F-009] stop power supply if turned OFF] [MF006] power is supplied if turned OFF	7	7							
	 switch electrical open	 [[F-008] provide power if turned ON] [MF005] no power is supplied if turned ON	1	1	N	 [produce coil] [MF014] mechanically broken coil is produced	0	 [1] periodic calibration of production equipment for coil	 electrical test - coil [det: 0]	0	0
 [F-008] provide power if turned ON	 [MF005] no power is supplied if turned ON	 [F-002] heat] [MF001] no heating	8	N	 [switch] switch electrical open	0					
			8	N	 [produce switch] [MF016] mechanically broken switch is being produced	0					

The close linkage between the FMEA form and the SysML model synchronizes all changes in the model structure immediately in the FMEA form. Even more, the hierarchical and component-oriented structure of the SysML model allows to derive event chains that track the effects of failures all the way up to topmost system level. Besides these benefits of a model-based approach also the reuse of FMEA data is fostered by applying the type/instance concept of SysML. For example reusable components along with their failure modes and the component internal effects chains can be organized in libraries and thus made available in other projects.

The SysML based FMEA method described here requires suitable tools for use in practice – otherwise the expected advantages - improved consistency and increased efficiency - cannot be achieved. Such an adequate tool does not only increase the acceptance of the method, but also prevents the FMEA from being perceived only as a time-consuming and disturbing but necessary additional activity to system development.

*Statistics from the Centre of Automotive Management in Bergisch Gladbach

Authors

Dr. Marc Born

Chief Technology Officer
KPIT medini Technologies AG,
Subsidiary of KPIT Technologies GmbH



Dr. Eckhardt Holz

Senior Advisor Functional Safety
KPIT medini Technologies AG,
Subsidiary of KPIT Technologies GmbH





About KPIT

KPIT medini Technologies is a part of **KPIT Technologies**. KPIT Technologies (BSE: 532400, NSE: KPIT), is a fast growing global product engineering and IT consulting partner focused on co-innovating domain intensive technology solutions for automotive & transportation, manufacturing and energy & utilities corporations. KPIT is at the forefront of automotive engineering globally with solutions in the areas of AUTOSAR & in-Vehicle Networks, Body Electronics, Chassis, Safety & Driver Assistance, Functional Safety, Vehicle Diagnostics, Infotainment and Powertrain.

Press Contact:

Melissa Womack

Tel: +12145050228

melissa.womack@kpit.com

www.kpit.com