ArchitectECA2030

SC 2 Demo 2.2 Key Card

Formal-Model-based Monitoring Device

Main aim

- *A monitoring device based on formal methods.*
- *Methods for quantifying residual risk and monitoring functionality as well as error correction.*

The demonstrator is physic simulation of a HV battery, including a virtual sensor model, and a thermal controller.

Partners	*INRIA, AVL, TUG*
ECS value chain	*Propulsion System / Tier 1*

State-of-the-art	Beyond SotA / Innovation	Targeted TRL
• *Predictive maintenance methods are available* • *Estimation of residual risk with statistics or physics-of-failure*	• *Formal-method-based residual risk estimation will be more accurate* • *Methods should be universally applicable to other components*	*TRL 4,* *TRL 5*

Link to project objectives

Objective	*Addressed (Y/N)*	*How*
O1 – Continuous robust design optimization for each part in the ECS value chain	*Y*	*Monitoring devices based on formal methods will enhance the robustness of components.*
O2 – Framework for safety validation of ECS value chain	*N*	
O3 – Identification & management of residual risks over the entire ECS value chain	*Y*	Multiple methods to estimate residual risk will be developed in this demonstrator. This gives us a chance to also compare different methods.
O4 – End-user acceptance by trustworthy ECS value chain	*N*	
O5 – Zero emissions, zero crashes, zero congestions by ECA2030-car	*Y*	The goal of the Monitoring Device is to warn the system before a crash happens, and therefore reduce the number of crashes, towards the goal of zero crashes.

Joint demonstrator (JDEM SC2)

DEM 2.1	DEM 2.2	DEM 2.3
SC	SC	SC

Linked supply chains (Y/N)

SC1	N
SC2	Y
SC3	N
SC4	Y

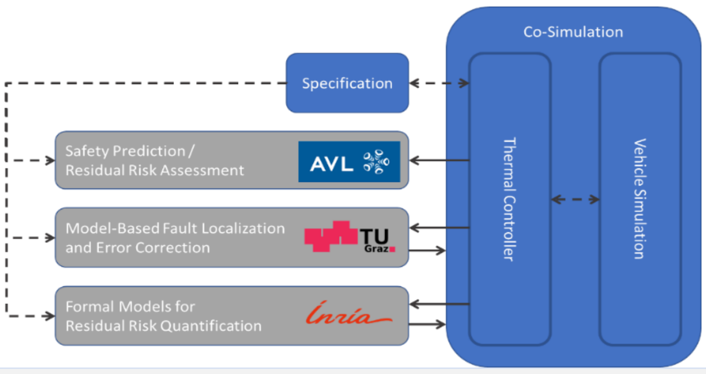
Considered MonDev layers (Y/N)

System (S)	N
Subsystem (SS)	N
Component (C)	N
Subcomponent (SC)	*Y*

Setup

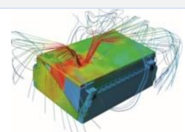
AVL will provide the Co-Simulation, including the thermal Controller and a vehicle simulation.
Furthermore, AVL will provide a method for safety prediction and residual risk assessment.

- *INRIA will exploit the thermal model's formal model for diagnosis and residual risk quantification.*
- *TUG will develop a fault localization and error correction method. Based on this method monitoring functionality will be provided.*



Benchmark scenario/mission/etc.

- *Finding errors in HV batteries itself is very critical as the HV battery is used for a lot of autonomous systems.*
- *The approach should be universally applicable to components of the propulsion system, which enables a wide range of V&V tasks.*



KPIs (related to requirements)

Functional completeness

- *The failure model should be correct in the predefined usage space*
- *KPI: Functional completeness by testing*

Model-based diagnosis for fault localization

- *The diagnostic model offers fault isolation and identification capabilities. Intermittent, incipient and novel faults should be considered.*
- *KPI: Model coverage*

Correction and reaction to diagnosed faults

- *For a diagnosed fault, the system provides an actionable strategy*
- *KPI: Classification error*

Baseline

Reliability

- *The failure model has to be more reliable than the SUT*
- *KPI: Divergence between failure model and SUT*

Real time online diagnosis

- *Faults have to be detected and diagnosed in real time. The sensors and interface must also be real-time capable.*
- *KPI: Latency*

Availability

- *The battery of the SUT needs to provide fast enough measurements such that the failure model can calculate the degeneration of the battery*
- *KPI: Availability of measurement data*

Evaluation

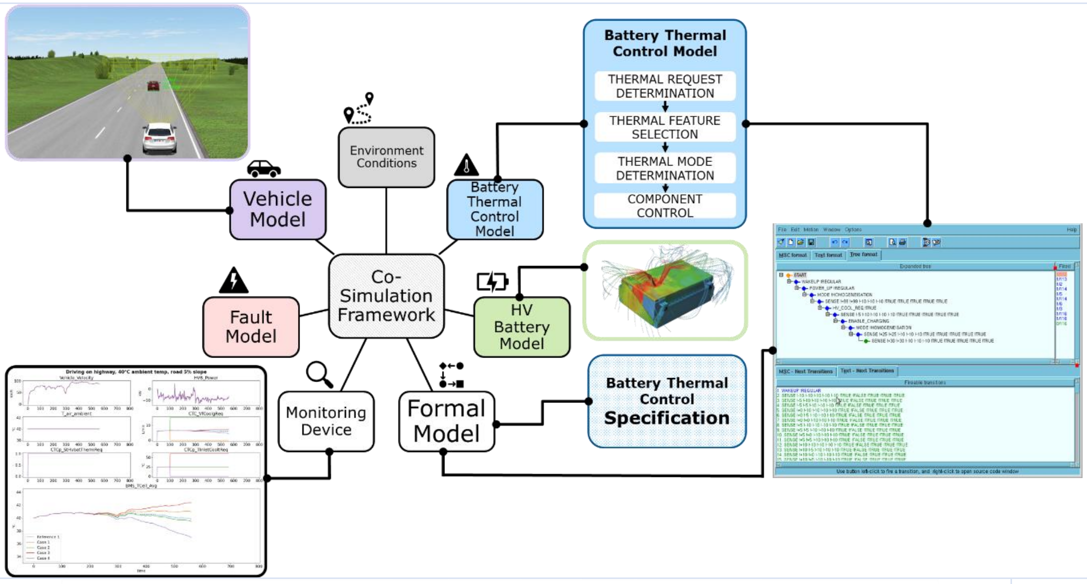
Evaluation platform will be a Co-Simulation framework including an ADAS/AD driving model, a HV battery model and a thermal control unit of the HV battery. In addition, the framework enables to add further methods and architectures as a Monitoring Device to perform diagnose calculations.

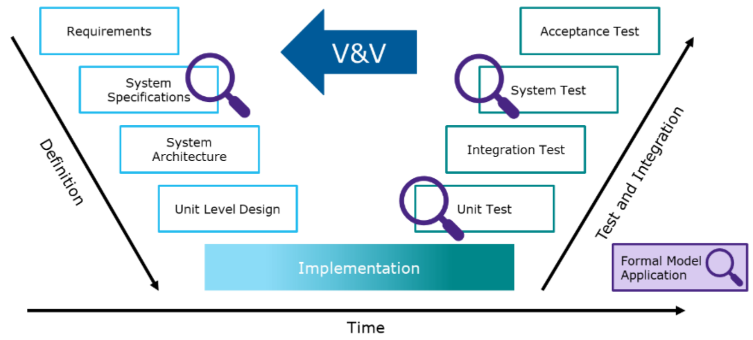
Current status/demonstration

- A FMEA table is generated to provide a detailed description and specification of possible faults in the HV battery system during operation or charging.
- Based on the FMEA table a fault injection model is developed to validate the formal model and model-based diagnosis approach.
- Formal model of the Thermal Control Unit is developed and validated - offline combination with the Co-Simulation framework by trace analysis.
- Probabilistic fault criticality estimation methods applied on the case-study.
- Completion of the formal model, requirements, and their verification.
- Submitted research paper.
- Development of Monitoring Device based on machine learning algorithm to identify an abnormal behavior of the system under test.
- **Simulations** are executed based on different conditions related to the introduced FMEA table for fault simulation in the thermal control unit.

Highlights and Conclusion

- Application of formal models reduces risks through detailed system specification analysis, capturing all requirements, models, and interpretations.
- The formal model serves as an abstract reference for the thermal controller, assuming all properties corresponding to requirements are met.
- Probabilistic analysis aids in selecting countermeasures by estimating the criticality of requirements and system faults.
- Formal models have limitations, including the inability to address unknown risks and properties beyond the operational domain.
- General health monitoring using a hierarchical concept (Task 3.3) is deemed necessary for advanced analysis, complementing the formal model's limitations.



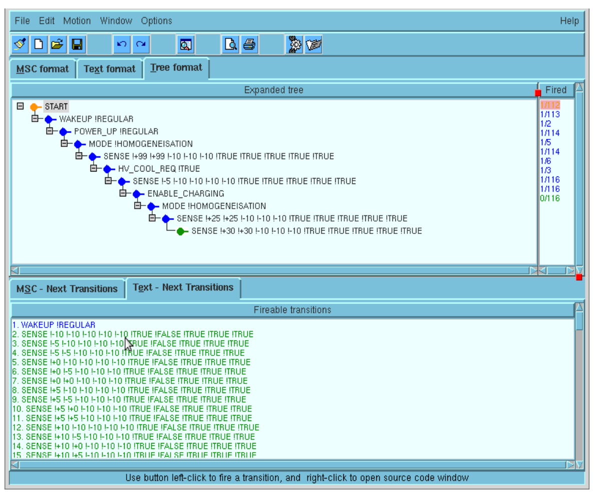


Model	Parameter for fault simulation	Input	Output	Value Type	Unit	Range	Signal/Parameter
Environment Conditions	Ambient temperature	X		float	°C	-30 → 50	Environment Setting
	Initial coolant temperature	X		float	°C	-30 → 50	
Vehicle	Velocity	X		float	km/h	0 → 200	Vehicle drive cycle & power request
	Acceleration	X		float	m/s^2	0 → 6	
	Road Profile	X		float	%	-20 → 20	
	Brake	X		float	m/s^2	0 → 10	
HV Battery	Cell temperature	X		float	°C	-30 → 60	Vehicle sub-component behavior
	Power max		X	float	kW	200 → 300 (peak) 100 → 150 (cont.)	
Thermal Controller	Cooling temperature	X		float	°C	-30 → 60	Vehicle sub-component behavior
	Cooling flow rate		X	float	L/min	0 → 20	

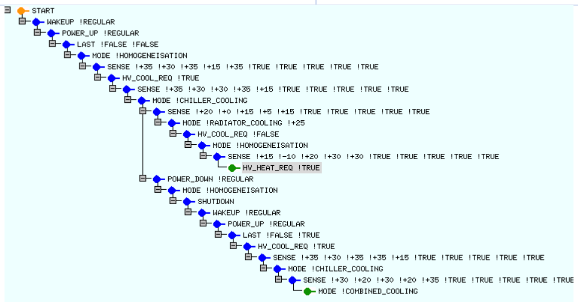
pav. 1: The table shows the available simulation enviornment paramter configuration to trigger different behavior of the overall system and in specific the thermal control unit.

HV Battery Fault	Consequences	Severity Risk	Explanation
Battery too warm	No electric driving	8	• Cooling system performance too low • Cell overtemperature • Component overheating • Improper filling
	Vehicle immobility	8	
	Release of toxic gases	10	
	Thermal event	10	
Inhomogeneous temperature spread inside the battery (hot spots)	Vehicle immobility	8	• Cell temperature spread is too high • Cell differential ageing
	No electric driving	8	
	Reliability not achieved	7	
	Durability / lifetime target not achievable	8	
Battery too cold during driving	Vehicle range not achieved	9	• Cooling system performance too low • Cooling system pressure drop too high
Battery too cold during charging	Vehicle range not achieved	9	• Cooling system performance too low • Improper filling
	Driving discomfort	4	
	Tool low pure electric range	7	
Component overheating	Vehicle immobility	8	• Improper filling • Cooling system pressure drop too high
	Durability / lifetime target not achievable	8	

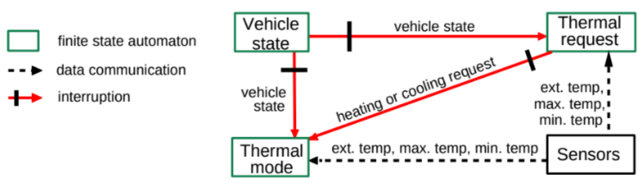
pav. 2: FMEA table with sevirity risk assesment showing possible single faults which could appear during operation in the HV battery system including the thermal control unit.



pav. 3: CADP software solution for validity check of the formal model based on the simulated traces of the high voltage battery system.



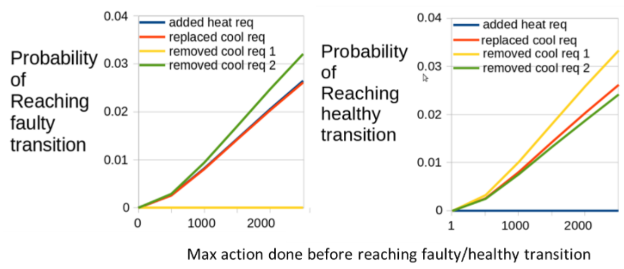
pav. 2: Step-by-step exploration of the formal model.



pav. 4: Formal model schema to show the specifications of one of the high voltage battery system tranistion states.

Requirements based analysis results

- Probability of reaching faulty (resp. healthy) action after at most MAX actions
- Results for 4 faults in the Thermal Request automation
- 1 addition, 2 removal, 1 replacement



Impact

Usage of formal model methods and model-based diagnosis to detect a faulty system during runtime. This offers a way to identify the residual risk and as well to minimize the risk of undetected faults.

Used standards

- *ISO 26262, ISO/PAS 21448:2019 (SOTIF), IEC 61508 (Eight parts 0-7)*

Future standardization potentials

- *Not perceived yet*

ArchitectECA2030 has been accepted for funding within the Electronic Components and Systems For European Leadership Joint Undertaking in collaboration with the European Union's H2020 Framework Programme (H2020/2014-2020) and National Authorities, under grant agreement n° 877539.

Demo Leader Contacts:
Company
Name, Surname, email.