# SACRED Step 2-

Step 2 of the SACRED methodology involves an exploration of the scenario definition with the express purpose of the identification of possible hazards and a classification into its core characteristics. Characteristics of hazards vary depending on the scope of the ODM and the environment, for example, a particularly rocky environment such as one in the Nordic countries would have a greater concern for rubble than the Netherlands. For our key example (Berlin, Germany) we consider the classifications within the context of Urban, Suburban and Rural as defined within our ODM as part of step 1.

## Characterization of Hazards

To begin the identification of hazards, we first must define what we are looking for, The ISO 26262 [1] defines a hazard as a potential source of harm. In PEGASUS [2], different sources of hazards for automated driving were distinguished, namely hazards arising from (1) the impact of the environment on the ADS, (2) the impact of the ADS on the environment and (3) the interaction between human driver and ADS. According to [3], a scene describes a snapshot of the environment, while a scenario describes the temporal development between several scenes in a sequence of scenes. Thus, a hazardous scenario can be characterized by adding contextual information to an identified hazard by means of environmental triggers. A comprehensive catalogue of such scenarios then enables a test-driven verification approach for automated driving.

Traditional approaches to Hazard Identification include HAZOP [4] a brainstorming methodology for hazard identification, Fault Tree Analysis (FTA) [5] which is the exploration of hazard cause in the form of branching tree diagrams and System-Theoretic Process Analysis (STPA) [6] which is the idea that a hazard is actually a sum of parts where untreated environmental influences interact with defects of components that lead to unsafe interactions within control loops, this leads safety to be more of an emergent property where a system interacts with components in a larger context, rather than assuring each part of the system as ‘safe’, ‘unsafe’ actions are instead identified and then constrained within the bounds of ‘safety.’ The classification of hazards within the SACRED methodology uses teachings from all of these traditional approaches and while other hazard identification approaches exist such as the Swiss cheese model of safety [7] and others, the beforementioned methods encapsulate the requirements of Step 2 well enough that it is best to focus on these teachings.

Within the Scenario Definition stage of SACRED Step 1, Environmental Levels are discussed, inspired by [8] Els are a classification of the relation between a hazard and the AS, with a closer relation being a higher level. Kramer discusses in his paper how hazards evolve over time, with the framing device of autonomous cars causing traffic in the event of hazard detection and correction, as discussed

When considering the classification of a hazard within SACRED, the key categories to consider are:

* Occurrence Rate

How often is the hazard expected to occur?

* Risk Rate

How bad is the hazard and how much harm does it pose to the system?

* Stakeholder Impact

Who does the hazard impact?

* Reaction Classification

Can we do anything about the hazard once it has been detected?

* Environmental Conditions

Division of the Scenario Definition into differing Environmental Levels where a hazard can occur

* Hazard Triggering Scenario

What is the causal chain of events that lead to a hazards occurrence? At what ‘Environmental Level’ is the hazard?

Citations:

1. ISO: ISO 26262:2018: Road vehicles - Functional safety (2018)
2. PEGASUS: Critical Scenarios for and by the HAD (2017). [www.pegasusprojekt.de/files/tmpl/PDF-Symposium/06 Critical-Scenarios-for-and-by-the-HAD.pdf](http://www.pegasusprojekt.de/files/tmpl/PDF-Symposium/06%20Critical-Scenarios-for-and-by-the-HAD.pdf)
3. Ulbrich, S., Menzel, T., Reschka, A., Schuldt, F., Maurer, M.: Defining and substantiating the terms scene, situation, and scenario for automated driving. In: 2015 IEEE 18th International Conference on Intelligent Transportation Systems, pp. 982–988. IEEE (2015)
4. L. Kotek, M. Tabas, HAZOP Study with Qualitative Risk Analysis for Prioritization of Corrective and Preventive Actions, Procedia Engineering, Volume 42, 2012, Pages 808-815, ISSN 1877-7058, <https://doi.org/10.1016/j.proeng.2012.07.473>.
5. The Fault Tree Handbook W. E. Vesely, U.S. Nuclear Regulatory Commission F. F. Goldberg, U.S. Nuclear Regulatory Commission N. H. Roberts, University of Washington D. F. Haasl, Institute of System Sciences, Inc
6. Leveson, N.G.: STAMP: an accident model based on systems theory. In: Systems Thinking Applied to Safety, Engineering a Safer World (2012)
7. James T. Reason – Revisiting the Swiss Cheese Model (2006) Project Safbuild – EEC Note No. 13/06
8. Identification and Quantification of Hazardous Scenarios for AD - Birte Kramer et al. Model-Based Safety and Assessment pp 163–178