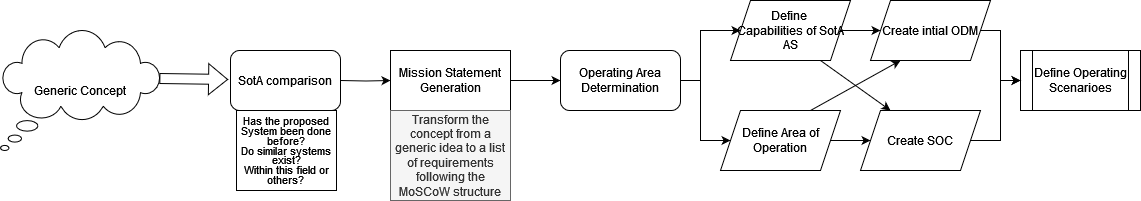
Step 1 of the SACRED methodology is pivotal in transforming a broad concept of an Autonomous System (AS) into a well-defined framework with clear objectives and parameters. This document focuses on the S-Bahn Berlin as a practical example to illustrate this process.

The primary goal of this document is to guide the reader through the process of deriving an Operational Design Model (ODM) and a Safe Operating Concept (SOC) from a conceptual idea of an autonomous railway system. By delving into the specific case of the S-Bahn Berlin's autonomy, we will outline the essential characteristics needed for the subsequent stages of the SACRED methodology. This includes a detailed justification of the decisions made and an initial exploration of the scenario to establish a foundational safety case.

Through this walkthrough, we aim to provide a clear and structured approach to conceptualizing and initiating the development of an autonomous railway system, setting the stage for the comprehensive safety assurance process that SACRED offers.

## From the State of the Art to a Mission StatementA diagram of a diagram Description automatically generated

At the outset of this methodology, we begin with a broad, overarching concept: “Create an autonomous railway system that can operate within X location.” It's important to note that if the concept provided already includes detailed specifics, you may bypass certain stages of this methodology that focus on developing those particulars.

### SotA determination

Our first step is to assess the current state of automation in contexts similar to 'X'. For our example, we are examining the state of automated rail systems in Berlin. This exploration helps us define our scope. By extending our investigation to similar urban hubs across Europe, we gain insights into the automation trends in high-density areas. Our research reveals that key focus areas in automation include Light Rail, Metro systems, Tramway systems, and potentially cross-country railways. Relating this back to Berlin, we can narrow down our interest to urban-based passenger light rail lines in densely populated areas and scope this further out to the operation within the Suburban and Rural areas of the S-bahn operation.

A short exploration into the state of the art regarding urban railway automation has been produced supplementary to this document, with the conclusion that automation has not been explored deeply within the domain of railway outside of countries such as China. (This would be part of the literature review.)

### MoSCoW Structure

With a clear understanding of the SotA, we are now positioned to articulate a mission statement. This statement will be structured using the MoSCoW method, which categorizes objectives into four categories: Must have, Should have, Could have, and Won't have. This structure ensures that our mission is aligned with realistic goals and priorities, reflecting the current technological capabilities and specific needs of urban rail systems like the one in Berlin.

“*The S-bahn Berlin is a lightrail system that operates within an urban capacity, recent development within lightrail has paved the way for the development of a GoA-4 urban system which detects anomalous activity through visualisation using front mounted cameras.*

*The AS must be able to detect large, static objects that will cause disruption, that is within its path on the track, furthermore, the AS must be able to determine what its path is through track extraction determining the key area of risk. The Scenario Definition must generate a list of environmental risks for the purposes of Physical Hazard Detection within step 2. The AS must be able to operate within at least a partial amount of the S-Bahn Berlin’s typical operation track within identification of ‘typical scenario.’ The AS must be theoretically sound as to be able to operate on technology that is identified as realistic within Step 6.*

*The AS should be able to identify moving objects on its track for the purposes of determining risk within step 2. The AS should be able to account for each object within the Scenario Definition and should understand the risks of translating physical objects to digital planes which should display itself within Digital Hazards present within step 2. The AS should be able to police itself regarding known knowns and known unknowns relevant to the scenario definition and Operational Design Model for the purposes of Criticality Determination within Step 4. The AS should be able to operate within a majority of the B-Bahn Berlin’s typical operation track within a non-perfect scenario, for example, non-disastrous weather which changes the visualisation of the track without altering it dramatically, weather that can be expected within the given climate, i.e rain or snow and operation within normal operating times, night or day. The AS should be properly represented within a simulated environment as defined within step 6.*

*The AS could operate within the entire operating area of the S-bahn Berlin within any operational capacity of weather, time of day or any extremity, given enough relevant data. The AS could classify Hazards not present within steps 2 or 3, given a wide enough operation time and support vector datasets. The AS could operate with technology greater than that that is to be identified within Step 6 through greater funding, more time for SotA development and more. The AS could theoretically operate on real equipment and within the real world within the parameters defined within Step 6, should the AS prove sound and be worth deployment.*

*The AS would have track-side visualisation within a scenario where that is determined the only possibility present itself, trackside detection has otherwise been determined frivolous within the concept specification given. The AS would operate with technology greater than that that is to be identified within Step 6 if these developments are to be made post deployment.”*

## Operating Area Determination

Following our mission statement, we now need to determine both of our initial limitations in the Operational Design Model and the Safe Operating Concept, the Safe Operating Concept researches the area of operation and identifies the “theoretical maximum risk” that the Autonomous System could encounter within “normal operation” before modelling this area and listing all risks associated with the scenario.

A close-up of a computer screen

Description automatically generated

### Safe Operating Concept

Discovering a Safe Operating Concept within a designated operational zone of an Autonomous System involves a process of exploring the area and isolating the segment with the greatest perceived risk. Within the example of the S-bahn Berlin, the entire route was examined, and the commute was separated into three separate zones of "Urban" "Suburban" and "Rural" with each having their own definition according to the SOC, this matches the official S-bhan route, as shown within the image below:

A map of a subway system

Description automatically generated

The investigation of the Urban zone of the S-bahn revealed a environment of mostly closed off high security railway systems where the likelihood of an incident being accidental is close to impossible, the railway system is completely closed from the rest of the city with high wire fences, clear area limitations at stations and is generally a “low-risk” area. The investigation of the Rural Zone revealed safety through seclusion. It is generally assumed that an area is low risk due to the low-density of population within the surrounding area, therefore, fencing is not needed; within this area, large sections of track are uncovered making this area a suitable target for theoretical incident explorations. The suburban section of the map is a suitable mix of the Urban and Rural stations; however, this fluctuation of safety means there is no identifiable area for risk determination quite as applicable as an area within the Rural development.

As part of the Safe Operating Concept, we must know the capabilities of the Autonomous System, for rail, the list of features needed is quite small; we only need know the Average Speed, Stopping Distance, Track Limitations, Weight and Reaction speed of the vision software.

From the above, we have identified a target as an area within the Rural section of the S-bahns route, through investigation, a 2km open section of track between Mahlsdorf and Strausberg Nord was identified, a route within 1km of farmland creates the hypothetical risk scenario of an issue with farmland perimeter allowing for the escape of farm animals followed by the possible roaming of a farm animal onto the track, judging by footage <https://youtu.be/MQePsZG8a9w?t=605> from the turn, there is ~15 seconds between gaining full vision of the straight and the clearing of the straight, knowing our stopping distance and average speed, that gives us ~2 seconds to react to something at the tail end of our vision, the process has been illustrated below:

A black and white ladder with a black flower

Description automatically generatedA drawing of a crosswalk

Description automatically generated with medium confidenceA diagram of a road

Description automatically generated

For our example, we immediately estimate all surrounding information of the real world, the AS has ~2 seconds to decide the best course of action so information such as the weather and object information are to be assumed for now. the trajectory of the object is assumed stationary, the object is kept as an unknown, the weather is assumed worst case scenario (rainy.) This “Worst case scenario” is to be expanded upon within Step 2, however, for now it serves as a model for what we can reasonably expect.

An exploration of what the decisions could be is also to be done within the initial ODM, as mentioned, the only variables of interest are “Size” (relative to the rest of the world, so inc weight) “Location” and “Reaction of train” (Stopping distance, reaction time and track limitations.) From this, we are able to map out all reactions within our initial operating scenario and display them within a Binary Flow Diagram as shown:

A diagram of a diagram

Description automatically generated with medium confidence

This Binary Flow Diagram and Scenario Definition is to then be used in order to create an initial Operational Design Model of the identified “complex environment” which will be re-defined within Step 4.

However, within the short term, the BFD and SD are used in order to define the Operating Scenarios to be explored within Step 2.

### ODM

An Operational Design Model (ODM) is a model of the world in which the AS can operate, it sets parameters where the AS can be defined as ‘safe’ when operating, traditionally it is not reasonable to expect the ODM to encapsulate the entire operating area of an autonomous system due to both the complexity of the world and the freedom of an autonomous system. However, a key feature of the SACRED methodology is its application towards railway development specifically, rail has a function that operation outside of the track is impossible, therefore, with adequate scoping, a fully realized ODM should be possible.

As explored within the SOC, a railway system has only three responses at any given time, to stop, to honk or to continue; therefore, any given scenario should generate a response within this scope. Being as the S-bahn Berlin has three classifications of operation, three separate ODM’s would be needed, however, the ODM for all SACRED applications should be close to uniform as railway operations do not differ to greatly from one another.

Any railway domain needs to consider the following:

1. **Geographical Environment**
2. **Infrastructure**
3. **Train Types and Specifications**
4. **Safety and Security** **surveillance**,
5. **Operational Protocols**.
6. **Weather and Environmental Conditions**
7. **Regulatory and Legal Framework**
8. **Technology and Automation**
9. **Passenger Services and Amenities**
10. **Traffic Management and Control**
11. **Maintenance and Inspection**.
12. **Economic and Commercial Aspects**
13. **Human Factors**
14. **Communication and Information Systems**
15. **Sustainability and Environmental Impact**

To classify as ‘safe’ and ‘functional’ the train needs to be able to get from station a to station b and allow passengers to evacuate if necessary. The railway system also needs to operate within the context of a functioning environment, which is where sustainability is concerned. For many instances, each definition will be static.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | Category | Rural Area | Suburban Area | Urban Environment | | Geographical Environment | Farmland, isolated areas, low population density. | Close to motorways, medium density housing, more accessible. | High-density areas, often underground sections. | | Infrastructure | Low to no fencing, basic stations, limited facilities. | Short brick walls, regular fencing, more developed stations. | Large concrete walls, sophisticated stations with extensive facilities. | | Safety and Security  \*unknown at this point\* | less surveillance due to isolation. | Enhanced security and surveillance, pedestrian crossings. | High security and surveillance, especially in underground sections. | | Operational Protocols | Less frequent service, adapted to local needs. | Regular service, integration with local transport networks. | High-frequency service, complex coordination with urban transport. | | Weather Conditions | Vulnerable to weather extremes, less infrastructure to mitigate effects. | Moderate vulnerability, some infrastructure for weather adaptation. | Largely unaffected by weather in underground sections. Overground should have quick turnover rate for response. | | Regulatory Framework  \*unknown at this point\* | Unknown at this time. | Unknown at this time. | Unknown at this time. | | Technology and Automation |  |  | Pre-existing implementation possible with low GoA infrastructure | | Passenger Services | Basic amenities, lower passenger volume. Emergency exit conditional | Emergency Exit reasonable | Emergency Exit risks underground lock | | Traffic Management | Simplified traffic management due to lower train frequency. | More complex traffic management, integration with road traffic. | Highly complex traffic management, integrated with urban mobility. | | Maintenance | Regular maintenance, challenges due to remote location. | Regular, more accessible maintenance facilities. | Frequent maintenance, specialized facilities for underground operations. | | Economic Aspects | Lower revenue, higher operational costs per passenger. Assess value of Automation? |  | High revenue potential, complex fare structures. Automation required for filling timetable gaps. | | Human Factors | Weather monitoring, track debris monitoring, timetable monitoring, route density monitoring |  |  | | Communication Systems | Basic communication systems, possibly limited due to remote location. | More advanced communication systems, integrated with local networks. | | Environmental Impact | Non-relevance due to structure pre-existing |  |  | |

It will be the automations job to identify if operation is within ODM or not at a given time, with protocol required should the ODM be exited, this is to be expanded upon within Step 6.

### Scenario Definition

With the ODM defined and the Safe Operating Context required, it is time to fully scope out the Scenario, within our case study, we are already aware of the separation between Urban, Suburban and Rural, however, each scenario is to be categorised further into Environmental Conditions, the relationship between the scenario and the AS classifies the level of the environment, for example, any railway system exists upon a railway track, meaning that regardless of application, Level 1 of the Scenario will always be the Railway Track, any hazards identified on a railway track within step 2 is to be classified as L1, above L1 is the system health itself, L0 where a system must be operational in order to be classified as autonomous, below L1 would be any additional levels of scenario, possibly traffic, signage, the road in which the track resides (in the case of urban trains) and so on. The Environmental Modelling system is inspired by “Identification and Quantification of Hazardous Scenarios for AD” by Zeller et al. Zeller introduces the Environmental Modelling system exploring how hazards can evolve between levels if left unchecked, an idea to be explored within Step 2 of SACRED.

## Operation Scenario Conclusion

As we progress to Step 2 of the SACRED methodology, it's crucial to adopt a comprehensive view of the railway system. This involves a thorough exploration of potential hazards and understanding where overlaps in hazards might occur across different scenarios. In our case study of the S-Bahn Berlin, we segmented the operating scenario into 'Rural,' 'Urban,' and 'Suburban' zones. This classification was based on the premise that similar sections of track within each category would, in theory, have comparable safety requirements.

However, it's important to note that at this stage, all classifications within the Operational Design Model (ODM) and Scenario Definition (SD) are tentative. They are formed based on informed assumptions and available resources. The validity of these classifications and the assumptions underlying them will be rigorously examined in Step 4 of the SACRED methodology. This step will be instrumental in verifying the initial hypotheses and ensuring that the ODM and SD accurately reflect the real-world scenarios and risks associated with each zone.

In summary, the work done in this initial step lays a speculative yet informed foundation, which will be critically evaluated and refined in the subsequent steps of SACRED, ensuring a robust and comprehensive safety assurance process for the autonomous railway system.

### Tech identification and passive exploration.

SACRED is a 7 step methodology wherein the actual exploration of technology doesn’t begin until step 6, however, within step 1, when generating the MoSCoW structure, features are identified that must be accomplished, within subsequent steps it is important to keep in mind that all identified traits (relevant hazards, requirements to assure and classification of hazard/criticality.) Will all need to be possible on some sort of Autonomous System, therefore, in order to not lose time or effort, it is important to ensure that every suggested quality is possible using the state of the art. It may be worth identifying and exploring relevant software prior to the exploration of step 6.