SACRED Example: D10 - Limitation Report

Josh Hunter

November 20, 2025

The following document is an example of SACRED [D10]. It is purposefully abstract to a degree of reference, taking a tertiary look at the hazards we have previously identified within our case study. In actuality, this document would consider hazards to a further level of depth and would consider a wider variety of hazards, consider an exploration of this size, to each sub-component found within step 2.6.

Within our example of [D8], we identify three hazards, those being a SPAR, a SPAD and Low Adhesion. These are purposefully abstracted for the purpose of both [D9] and [D10], as we know from both [F] and [G], SPADs and SPARs are incredibly vague terms. As shown within step 2.6, a 'SPAD' is an umbrella term for a lot of faults; however, for the context of the Limitation Report, we are going to do a high level analysis of a SPAD and discuss what limitations arise from that.

Within [D9] we classify a SPAD as 'a SPAR which has posthumously been declared a danger due to an incident occurring.' The paper 'Railway signals passed at danger: A bibliometric analysis' by Ambhore, Sangiorgio and Weide classifies a SPAD as *'an incidence that narrowly missed becomes fatal when trains or trams erroneously exceed their movement authorities usually by intruding on stop signals.'* This definition has two important specifications, firstly, it declares that a SPAD must be a narrow miss of fatality, the second, frames a SPAD as a purely ego-fault due to the 'erroneous exceeding of movement authorities.' Although the paper later clarifies that a SPAD is much more systematic than it first seems, when considering a SPAD, we must take this naive approach so that we can properly scope out our limitations. Regardless of whatever system we have in place, our first limitation is our movement authority.

Movement authority within rail refers to the trains permission to move to a specified location based on a distance and speed profile, it is dictated by the status of a signal, the context provided by timetabling and the geography of the environment. So, based on this abstracted example, we have the limitations that our system must not encroach upon the timetable of any other train, we have to be able to physically see the signal, given the layout of the environment and we cannot pass the signal. However, if a SPAD has occurred, one of these limitations has been breached. We will explore what exactly a breach means within Step 4.