(4) checklists and expert judgement are frequently used for evidence assessment, and (5) significant research effort has been spent on techniques that have seen little adoption in the industry.

For a realistically large system, practitioners need to collect and manage large quantities of safety evidence throughout the analysis, development, verification, maintenance, operation, and evolution of the

system. This vast information has to be structured to show how it meets the requirements of a safety standard. If the evidence is not structured properly, its sheer volume and complexity can jeopardize the clarity of the satisfaction of the high-level safety objectives [8]. Safety evidence can be structured either graphically (e.g., with models) or textually.

The system supplier thus has to keep track of the various relationships in the body of evidence in order to be able to analyse change impact. This analysis aims at identifying the potential consequences of a change, or at estimating what needs to be modified to accomplish that change [10].

Although safety standards provide some guidance for managing safety evidence, they are generic and are typically large documents containing hundreds of pages and thousands of requirements [11]. For example, IEC 61508 – one of the most widely used safety standards – is organized into eight booklets (parts) with over 450 pages of text. For most safety standards, some degree of interpretation is required to tailor them to the context of application. This means that the system supplier has to decide based on the standard’s guidance what type of evidence is best suited for a given scenario, and how it should be structured, assessed, and managed. Therefore, standards do not necessarily reflect industrial practices in safety evidence management, but only provide general information about practices that may be employed. This implies that the standards do not allow someone to know if certain practices are used, or to determine their frequency of use.

Despite the abundance of research focused on supporting and improving safety evidence management,few publications have been validated in real industrial projects or have provided empirical evidence about practices and perspectives in the industry.

2.Reliability Engineering and System Safety

In this work, we focus on two groups of stakeholders, namely certiﬁcation author- ity auditors and development teams. Auditors could use the trend of the data over the history of a project lifecycle to identify software problems and possibly misleading information. The data could also used by the development teams within aerospace companies to assess the readiness of a software project against the certiﬁcation targets.

It is likely for software and safety engineers to over- or under-engineer the software in their effort to fulfill the requirements of the standards. To this end, they may over- spending to achieve certification credit or under-spending and risking an audit failure. An aerospace company can seek advice from the certification authorities, but, to maintain their independence, the authorities are restricted in the advice they can offer.

DO178B Lifecycle Data.

Plan for software aspects of certiﬁcation Design description

Software development plan Source code

Software veriﬁcation plan Executable object code

Software conﬁguration management plan Software veriﬁcation cases and procedures

Software quality assurance plan Software veriﬁcation results Software requirements standards Software life cycle environment Software design standards Conﬁguration index

Software code standards Software conﬁguration index

Software accomplishment summary Problem reports

Trace data Software conﬁguration management records

Software requirements data Software quality assurance records