Safety Evidence Traceability: Problem Analysis and Model

Sunil Nair[1], Jose Luis de la Vara[1], Alberto Melzi[2], Giorgio Tagliaferri[3], Laurent de-la-Beaujardiere[4], and Fabien Belmonte[4]

[1] Simula Research Laboratory, Norway
[2] Centro Ricerche Fiat S.C.p.A., Italy
[3] Rina Services S.p.A., Italy
[4] Alstom Transport, France
{sunil,jdelavara}@simula.no, alberto.melzi@crf.it,
giorgio.tagliaferri@rina.org,
{laurent.de-la-eaujardiere,fabien.belmonte}
@transport.alstom.com

Abstract. [**Context and motivation**] Safety evidence plays an important role in gaining confidence in the safe operation of a system in a given context. For a large system, it is necessary to provide information about thousands of artefacts that might be used as evidence and about the relationships among themselves and also with other safety assurance assets. [**Question/problem**] Past research has only addressed some needs of traceability in safety-critical systems and thus has not provided a complete picture of safety evidence traceability. Lack of knowledge and awareness of these needs can result in poor evidence management and lead to certification risks. [**Principal ideas/results**] This paper aims to provide a broad overview of safety evidence traceability needs for practice and its associated challenges. We also propose a safety evidence traceability model, which has been validated with data from real-world critical systems. [**Contribution**] We discuss the motivation and challenges for safety evidence traceability, and present the various traces that need to be captured and maintained. This information can help researchers to shape future research based on industry needs and can help practitioners to gain a deeper understanding and a wider knowledge of safety evidence traceability, thereby facilitating safety assurance and certification.

Keywords: Safety evidence, Traceability, Safety assurance, Safety certification, Safety Standard, SafeTIM.

1 Introduction

Critical systems in many domains are subject to a rigorous assessment or assurance process through which the system is deemed safe for a particular context. Such assessment process is usually based on the fulfilment of the requirements of some safety standard. To comply with a standard, system suppliers have to gather and present evidence information supporting their claims about system safety. We define

C. Salinesi and I. van de Weerd (Eds.): REFSQ 2014, LNCS 8396, pp. 309–324, 2014.

safety evidence as *"artefacts that contribute to developing confidence in the safe operation of a system in a given environment"* [1]. Some generic examples of safety evidence are test results, system specifications, and personnel competence. Such artefacts are used to support claims about system safety, and to show compliance with a standard.

For a realistically large system, a system supplier needs to collect and manage a large quantity of safety evidence throughout the analysis, development, verification, maintenance, operation, and evolution of a system. The system supplier must also capture and maintain traces between pieces of evidence information and also from and to evidence and other safety assurance assets (claims, arguments, etc.) in order to be able to demonstrate system safety.

In software engineering, traceability can be defined as the degree to which a relationship can be established between two or more products of the development process (aka artefacts), especially products having a predecessor-successor or master-subordinate relationship to one another [2]. With the above definition in mind, we define safety evidence traceability as *"the degree to which a relationship can be established to and from artefacts that are used as safety evidence"*.

Lack of knowledge and understanding of safety evidence traceability needs can result in improper evidence management, which may indirectly result in certification risks [3]. A system supplier might not be able to demonstrate system safety if the evidence is not well managed and traced. Consequently, a third party certification authority would not gain enough confidence in the safe operation of the system.

Although traceability for safety-critical systems and more concretely safety evidence traceability have been addressed in past research, no study has yet provided a broad and complete picture of safety evidence traceability needs. Most of the research has only focused on the relationships between the artefacts used as evidence (e.g., [4]). The studies that have explicitly or implicitly studied other aspects of safety evidence traceability have not paid much attention to many necessary relationships for evidence traceability. For example, works that have dealt with the relationship between safety evidence and the argument that justifies evidence validity for a claim (e.g., [5]) have usually not paid attention to other traces such as to artefact versions.

This paper aims to present an in-depth analysis of safety evidence traceability needs and its challenges that would be helpful for both researchers and practitioners. Based on others' past work, on our knowledge about the state of the art and practice (e.g., [6][1]), and on own experience in safety assurance and certification projects, we discuss the motivation for safety evidence traceability and its challenges. We also present the traces that must be created and maintained from and to evidence information. As a result, we have created a Safety Evidence Traceability Information Model for safety evidence - SafeTIM.

The results presented in this paper are part of the on-going work in OPENCOSS (www.opencoss-project.eu), a large-scale European research project on safety assurance and certification in the automotive, avionics, and railway domains. Beyond the usefulness of the results for the project, we consider that the contribution of the paper is twofold. Firstly, the problem analysis presented and SafeTIM can help researchers to better understand safety evidence traceability needs in industry and thus to identify aspects that might require further study. Secondly, practitioners can benefit by gaining awareness of important aspects related to safety evidence traceability

whose management can be essential for safety assurance and certification, thereby improving project management and reducing cost.

The rest of the paper is organised as follows. Section 2 presents the background of the paper. Section 3 discusses the motivation for safety evidence traceability. Section 4 describes the safety evidence traces, and presents SafeTIM and its validation. Section 5 compares SafeTIM with other models and discusses the challenges for safety evidence traceability. Finally, Section 6 presents our conclusions.

2 Background

This section introduces a common certification framework that is being developed in the OPENCOSS project and reviews related work.

2.1 Common Certification Framework

The main technical objectives of OPENCOSS are to (1) devise a common certification framework for railway, avionics, and automotive industries, and (2) establish an open-source safety certification infrastructure.

The common certification framework will consist of several, linked metamodels, each aimed at modelling different aspects of compliance [7]: (1) the safety standards followed; (2) project-specific aspects such as the actual process executed, the artefacts managed, and the argumentation used to justify the key decisions made; (3) the terms used in different safety standards and projects, and; (4) mappings between different standards and projects, in order to support cross-standard/domain certification.

Some of these models have been already published (for e.g., [7]), while others are accessible only for the project members. However, SafeTIM corresponds to a fragment of the large framework. The model presented in this paper contains the set of fundamental concepts and relationships for safety evidence. It must be noted that more information might be necessary in a safety assurance and certification project for other purposes (e.g., for assessment of process-based compliance). We believe that SafeTIM is an underlying model that lies behind the common certification framework and needs to be explicitly modelled to deal specifically with safety evidence traceability.

2.2 Related Work

Traceability has been an important research topic in software engineering during the last two decades. Despite the acknowledged higher importance of traceability for safety-critical systems [8], literature reviews [9][10] have shown that the ratio of papers on the subject is low.

Publications presenting and discussing the motivation (e.g. [11]), challenges (e.g., [12]), and open issues (e.g., [13]) for traceability are available in the literature. Studies on traces (e.g., [14]) and types of traces (e.g., [15]) can also be found, mainly in relation to traceability to and from requirements. Past work have also focused on strategic traceability needs and challenges specific to safety-critical projects [8].

What differentiates this paper from most of the past research on traceability is its focus on safety evidence. The number of publications addressing safety evidence traceability in isolation is limited, and there are few studies that discuss the needs and motivation of such traces [16][17]. For example, the literature on safety evidence traceability needs for evidence reuse is very limited. Given its importance for cost reduction in the development and assurance of new safety critical systems, we considered that it is an area that needs to be further investigated. Furthermore, these pieces of work have a very narrow scope (e.g., specific to a domain or safety standard) and do not provide a complete overview of the motivation and challenges regarding evidence traceability.

Most of the existing studies on traceability for safety-critical systems have focused on traceability between the artefacts resulting from their analysis and development, such as requirements and hazards [18], requirements and components [16], requirements and design [19], or requirements and code [17]. These artefacts and the traces between them can themselves be used as safety evidence. Models including a larger number of artefacts to trace have also been proposed [4][20]. Some papers have focused on traceability for specific safety standards (e.g., DO-178B [21] and ISO26262 [22]) or have modelled entities and relationships that abstract concepts common to different safety standards [7]. However these studies have not dealt with some specific traces to and from safety evidence that will be discussed in Section 4.1. With regard to safety evidence as an element of an assurance or safety case, the traces most frequently studied are with arguments and claims (e.g., [23]).

Some recent works have broadened the scope of safety evidence traceability. SACM (Structured Assurance Case Metamodel; [24]) includes an evidence metamodel that specifies relationships between evidence items and between evidence items and other assurance assets. The link between evidence and the process from which it results is addressed in [5]. An evidence-related conceptual model for IEC61508 with relationships beyond those between artefacts used as evidence [25] and a generic evidence model for safety cases [26] have also been proposed. Although these works have provided valuable insights, they still lack details about safety evidence traceability and their results do not meet all the needs presented in the next section (e.g., the purpose of the traces beyond safety assurance and certification).

Despite the limitations identified in the past research and the fact that no single study that has yet provided enough insights into safety evidence traceability in specific, our review of related work has helped us to better understand safety evidence traceability. As a result, we aimed to build and present in this paper SafeTIM - a holistic safety evidence traceability information model that synthesises traces indicated in the past work on evidence traceability and also deal with aspects that have not addressed in depth yet (e.g., evidence reuse).

3 Motivation for Safety Evidence Traceability

This section presents what we regard as the main reasons for safety evidence traceability: safety assurance, compliance with safety standards, change impact analysis, evidence reuse, and project management. Although some authors [11] have suggested that safety assurance and compliance with safety standards are the main

reasons for traceability in safety-critical systems, empirical evidence indicates that other motivations exist too [6].

Some of these motivations such as safety assurance and compliance with safety standards are specific to safety evidence or for safety-critical systems, while the others might be motivated from generic traceability needs. Nonetheless, these generic traceability needs are especially important for safety critical systems because of their rigorous and stringent certification context and the high costs associated to them.

It must be noted that the aspects discussed below are not exclusively independent, but rather related to one another (e.g., evidence reuse and change impact analysis). This also applies to the challenges discussed in Section 5.2.

M1: Safety assurance. A fundamental criterion for any safety-critical system, regardless of having to comply with some specific safety standard, is to ensure that its hazards have been avoided or mitigated. This allows gaining confidence in the overall safety of the system. Maintaining traceability of the evidence information involved is essential for this purpose so as to show that hazard mitigations have been properly developed and validated. For example, safety requirements can be specified from hazard identification and for their mitigation, and their satisfaction can be later verified with techniques such as formal methods.

M2: Compliance with safety standards. In domains such as avionics and railway, safety-critical systems must comply with safety standards for certification purposes. Therefore, system suppliers have to show fulfilment of the requirements of the standards. Traceability can be a means for this activity. In addition, system suppliers might have to explicitly provide traceability specifications as a part of the information that constitutes evidence of compliance [6]. Indeed, some standards mandate this information (e.g., DO-178C [27]).

M3: Change impact analysis. Changes in a safety-critical system and thus in its safety evidence are practically inevitable [28]. Practitioners must ensure that such changes in the system will not have any undesired effect in system safety and in the body of safety evidence. Therefore, such changes have to be managed adequately. For example, it is necessary to assess how a change in a piece of evidence might affect others [6]. Safety evidence traceability is necessary to perform such an impact analysis in order to identify the potential consequences of a change or to estimate what needs to be modified to accomplish a change.

M4: Evidence reuse. Reuse of a safety-critical component (or system) and thus of its evidence is important in industry [6], mainly in order to increase the return on investment in component development and to decrease system cost. However, it must be ensured that evidence reuse is adequate [28], or that a change in a reused piece of evidence is propagated to other uses when considered necessary. Maintaining safety evidence traceability supports evidence reuse and the execution of the associated required activities.

M5. Project management. Project management information such as that related to cost, effort, or degree of compliance is essential to make informed decisions during safety-critical system lifecycle. These decisions can be hard to make without adequate

safety evidence traceability. For example, it allows the estimation of the cost of a possible change, and helps practitioners decide whether the change should be implemented or not.

4 Safety Evidence Traces

This section introduces the various traces necessary to create and maintain for safety evidence traceability. We represent these traces graphically in SafeTIM, the traceability information model for safety evidence that we propose.

4.1 Traces to Create and Maintain

Based on (1) the analysis of the motivation for safety evidence traceability in the previous section, (2) the traces that we have identified in previous work, and (3) our knowledge and experience, we present the set of traces that we regard as necessary for safety evidence. Nonetheless, we acknowledge that, depending on their purpose, some practitioners might not need all of the traces for a specific project, or would require other specific traces that are not mentioned below. The overall motivation that drives each trace is mentioned in brackets.

Between Artefacts (M1, M2, M3 & M5). Traces must be created between the artefacts managed during system lifecycle such as a requirements specification and test cases. For those artefacts used as safety evidence, the traces between them can result in a chain of evidence [27]: a series of related pieces of safety evidence. However, traces could also be maintained to and from artefacts for purposes different to safety assurance or compliance [6]. For example, one might need to trace artefacts for change impact analysis. Traces between artefacts can also be used for project management. For example, requirements that have not been tested can be determined.

Between Safety Evidence and Claims (M1-M5). Safety evidence is inherently targeted at supporting claims about system safety and thus at gaining confidence in it. When evidence changes, the confidence in the related claims can vary. Confidence in safety evidence can also vary if a claim changes. Traceability between evidence and claims support evidence reuse when similar or the same claims are made, for instance, in different projects. Analysis of the claims for which safety evidence exists is also part of project management. When a claim refers to requirements of a safety standard, the related evidence aims to show compliance.

Between Safety Evidence and Arguments (M1-M5). Safety evidence alone might not be sufficient to gain confidence in a claim [26], and a justification might be necessary. Such a justification can take the form of an argument [23], which can clarify and substantiate claims based on safety evidence. When safety evidence changes, an argument might be affected, and likewise evidence might have to be revalidated when an argument changes.

Between Artefacts and Reference Artefacts (M2 & M5). Safety standards usually prescribe types of artefacts (i.e., reference artefacts) that have to be produced to show compliance. Practitioners must show how the concrete artefacts produced in a project materialise the reference artefacts. For example, DO-178C requires the creation of a reference artefact called Software Verification Results. Such a type could be materialised in a project by means of, for instance, a specific review (of requirements, code, etc.).

Between Pieces of Safety Evidence in Relation to a Claim (M1 & M3). Safety evidence traced to a claim could not only help gain confidence in its satisfaction, but could also make one lose confidence in the claim [24]. For example, a review could be used as a piece of evidence to support a claim about requirements accuracy, but other pieces of evidence (e.g., reviewer competence) could be used to show that not enough confidence exists in the accuracy. A relationship between two pieces of evidence can be created in order to specify that one supports or challenges the other in relation to a same claim.

Between versions of an Artefact (M1 & M2). An artefact can be modified, making a new version of a previous one. Maintenance of traces between the versions of an artefact can be necessary for safety assurance and even mandated by a safety standard. For example, it might be necessary that the versions of two related artefacts are consistent (e.g., because of temporal constraints), and configuration management practices can be required [6].

Between (re)uses of an Artefact (M3 & M4). An artefact used in a project (e.g., as evidence) can be reused to support different claims in the same or in a different project. Maintaining traces between these uses is necessary mainly for change impact analysis. Modification of an artefact in some of its uses might affect the others. For example, a new fault could be identified in a component used in one project and the same component might have been used in different projects. This trace would help to identify all the projects in which the component has been used and would allow the system supplier to change the required artefacts accordingly. It is also especially important to keep these traces when the artefacts reused are duplicated.

Between Artefacts and Activities (M2, M3 & M5). Artefacts are the result of the execution of some activity [25]. For example, test results can be produced in some validation activity. It is necessary to trace artefacts and activities so that practitioners can (1) identify the activities that might have to be re-executed due to artefact modification, and (2) show that they have executed the activities mandated in a standard. At the same time, this trace can also act as a measure to keep track of activities that have not yet been executed in a project.

Between Artefacts and Techniques used to Create Them (M1, M2 & M5). For safety assurance, an essential aspect of the artefacts managed in a project is to know how the artefacts have been created. More concretely, it is necessary to know the means (i.e., the techniques) used. Safety standards sometimes specify the techniques that should or must be used to create some artefacts. In many regulatory contexts,

system suppliers are not completely free to use a given technique unless they justify the suitability of their selection.

Between Artefacts/Pieces of Evidence and Provenance (M1, M3 & M5). Traces between artefacts and the information about their management (who created it, when it was created, artefact evaluations, etc.) can be very important for safety assurance [24]. This information can also help practitioners to decide on who should deal with changes in an artefact. Pieces of evidence can also have provenance information (e.g., who approved it).

4.2 SafeTIM: A Traceability Information Model for Safety Evidence

Based on the traces identified, we propose a traceability information model for safety evidence called SafeTIM. The model is shown in Fig. 1 in the form of a class diagram. The importance of explicitly creating a traceability information model for safety critical projects has already been highlighted in past research [8].

The definition of each class is based on past work. Every class has a unique identification attribute (ID) for implementation purposes [4][8]. SafeTIM classes are defined as follows.

- ***Artefact*:** Individual, identifiable units of data managed (used, modified, and/or produced) throughout system lifecycle [8][24].
- ***Piece of Evidence*:** The use of an artefact as evidence for a claim [24].
- ***Claim*:** Propositions being asserted in relation to system safety (or other safety-related system properties) [24][29].
- ***Artefact/Evidence Provenance*:** Characteristics of artefacts (or pieces of evidence) that correspond to information related to their lifecycle and the responsibility for their management [24].
- ***Project*:** An individual or collaborative enterprise [29] for system assurance or certification and in which artefacts are managed [24].
- ***Version*:** A particular form of an artefact differing in certain respects from an earlier form or other forms [24][29].
- ***Argument*:** A body of information (or reasons [29]) presented with the intention to establish one or more claims about system safety through the presentation of related supporting claims, pieces of evidence, and contextual information [24]. In essence, an argument aims to justify the validity of a piece of evidence for a claim.
- ***Participant*:** A party involved in the management of an artefact or piece of evidence [29].
- ***Artefact Relationship*:** This class represents the existence of a relationship and thus of a trace between two artefacts [30][12]. A relationship can be recorded in an artefact if the relationship itself is used as evidence (e.g., DO-178C explicitly requests the provision traceability information). Examples of types of relationships between artefacts (e.g., with regard to the content, abstraction, or evolution of an artefact) can be found in [24][12][14].

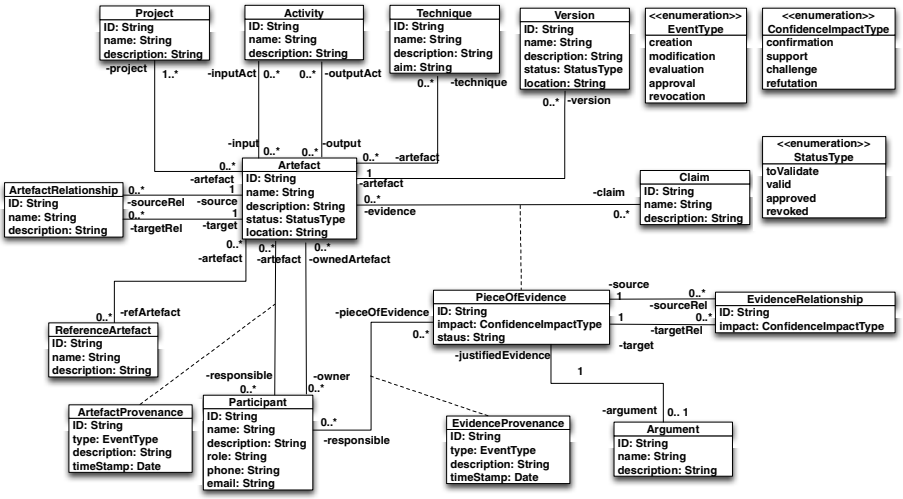

Fig. 1. SafeTIM – A Safety Evidence Traceability Information Model

- ***Evidence Relationship*:** This class represents the existence of a relationship and thus of a trace between two pieces of evidence in relation to the confidence in the validity of one of the pieces according to the other [30][24][12].
- ***Reference Artefact*:** Types of unit of data that a safety standard prescribes to be created and maintained during system lifecycle. Reference artefacts are materialised in assurance projects by means of (concrete) artefacts [30]. This means that these artefacts have the same or a similar structure (syntax) and/or purpose (semantics) [4].
- ***Activity*:** A unit of work that requires, modifies and/or produces artefacts [24] and corresponds to something being performed in system lifecycle [29]. Activities can be defined at different degrees of granularity (process, phase, task, etc.).
- ***Technique*:** A specific procedure through which a particular way of creating an artefact is accomplished [29].

  There are also three enumerations in SafeTIM.
- ***Event Type*:** This enumeration corresponds to types of events that can occur in the lifecycle of an artefact or piece of evidence [24][29]. Its literals are:
  - *Creation*: When an artefact or piece of evidence is brought into existence.
  - *Modification*: When a change is made in some characteristic of an artefact or piece of evidence.
  - *Evaluation*: When an element is assessed or evaluated.
  - *Approval*: When an element is accepted as satisfactory or as valid.
  - *Revocation*: When an element is cancelled or withdrawn.
- ***Status Type*:** This enumeration corresponds to the status of an artefact or piece of evidence, for instance, after a change in some related information. Its literals are:

  - *To Validate*: The validity of the artefact or piece of evidence has to be determined.
  - *Valid*: The artefact or piece of evidence is regarded as adequate for safety assurance and/or certification, but it still has to be approved.
  - *Approved*: The artefact or piece of evidence has been evaluated as valid, and not further evaluation is necessary unless some change takes place.
  - *Revoked*: the artefact or piece of evidence has been cancelled, withdrawn or revoked.
- ***Confidence Impact Type*:** This enumeration corresponds to the types of confidence in the validity of one evidence element as a result of the existence of another evidence element. Its literals are:
  - *Confirmation*: The validity of an evidence element is confirmed or established because of the existence of another evidence element.
  - *Support*: The validity of an evidence element is supported or provided by the existence of another evidence element.
  - *Challenge*: The validity of an evidence element is challenged or disputed by the existence of another evidence element.
  - *Refutation*: The validity of an evidence element is proven to be wrong because of the existence of another evidence element.

4.3 Model Validation

We developed SafeTIM with close reference to the results obtained from two large previous studies: a systematic literature review (on 216 publication) on the state of the art [1] and a survey (with 52 participants) on the state of the practice [6] concerning safety evidence management. In addition, most of the authors of this paper have extensive experience in safety assurance and certification in industry. Although the creation of the model based on our own knowledge and experience could be regarded as an implicit validation, we have performed further explicit validation.

The validation presented in this paper corresponds to the review of documentation (and artefacts) from real safety assurance and certification projects. These reviews were aimed to identify information in the documentation that map to the structure of SafeTIM. This way, we could explicitly validate that SafeTIM concepts and relationship have been used in real projects.

For the validation, we reviewed the following documentations:

- A synopsis of several safety studies and system specifications (e.g., safety requirements) of a sub-system targeted at complying with ISO26262 [31] in the automotive domain.
- The system safety case from a railway project that was certified against CENELEC standards [32].
- The system safety case, the safety plan, two sub-system safety cases, two hazard logs, several safety studies (e.g., the preliminary hazard analysis), several system specifications (e.g., requirements and design specifications), several V&V (verification and validation) plan reports (e.g., test procedures), several V&V results reports (e.g., testing results), and several safety certificates

(which correspond to the approval for executing some activity) from another railway project that was also certified against CENELEC standards.

We provide the following information about the documentation reviewed in order to show the size of the projects. For the sub-system of the automotive domain, the safety studies had a number of hazards that were mitigated and traced back to around 50 specific safety requirements. For the first railway project, the safety case consisted of almost 200 pages. For the second railway project, the safety plan consisted of over 35 pages. One of the hazard logs contained over 500 entries and over 2,500 traces from safety requirements to other six different types of artefacts. A typical example of the type of the railway projects has around 10000 requirements. More specific details cannot be provided for confidentiality reasons.

The main findings from reviewing these projects are as follows:

- All the classes and relationships of SafeTIM could be identified in several artefacts.
- In some cases, SafeTIM information was not explicit in the artefacts. For example, the safety cases did not explicitly contain information regarding arguments. However, arguments for justifying the use of an artefact as evidence could be extracted from the safety cases.
- We did not find any examples of counter-evidence (i.e., confidence impact corresponding to *Challenge* or *Refutation*). The reason could be that the documentation we reviewed corresponded to the final artefacts used to show system safety for the projects. However, we believe that practitioners should consider counter-evidence for their claims for reasons such as avoiding confirmation bias [33]. We neither found artefacts or pieces of evidence that were revoked, probably for the same reason.
- The companies had their own defined event types, but they can be mapped to those proposed in SafeTIM.

It must also be noted that the terminology used in SafeTIM is not exactly the same as the terminology used in some domains or safety standards. For example, the concepts of work product in ISO26262 or data item in DO-178C correspond to *Artefact* in SafeTIM.

In addition to the above documentation, we have also reviewed examples of safety evidence information in related work (e.g., [26]) and in OPENCOSS deliverables (e.g., [34]) to validate SafeTIM. We have also checked different safety standards (e.g., [27][31][32]).

Fig. 2 shows an illustration of the use of SafeTIM based on the information of one of the railway projects. The figure corresponds to an instance of SafeTIM. The information presented in the figure is generic and corresponds to the sanitised version of real data for publication purposes due to intellectual property constraints. Nonetheless, we believe that the illustration is sufficient to show one example of how the elements and relationships of SafeTIM correspond to the information of a real safety assurance and certification project.

In the example, the *Artefact* safety plan has a relationship to the *Claim* made about the description of the methods used to ensure that the safety goals are met. The artefact therefore is used as *evidence* for the particular claim with a confidence impact

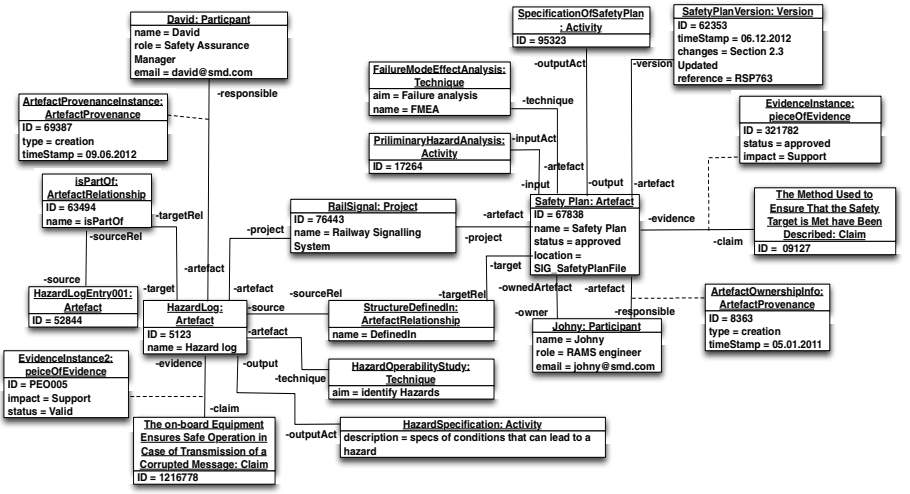

Fig. 2. Instance of SafeTIM concepts and relationships from a railway project

type *Support*. The safety plan is produced as a result of the *Activity* specification of the safety plan. The safety plan is used as input in the *Activity* preliminary hazard analysis. Apart from the activity, specific *Techniques* such as failure mode and effect analysis are employed in the project to give create artefacts. The model also shows some relationships between several artefacts. For example, a specific *Artefact* namely hazard log entry is part of the hazard log. The structure of the hazard log is defined in the safety plan. Since the example illustrates the information reviewed from one railway project, all the artefacts are managed by the same *Project*. Every artefact has *Provenance* information such as who created it and when, who owns it, and what is the role of the person involved along with contact details. Some artefact had versions in this example, as shown in the figure.

5 Discussion

In this section, we compare SafeTIM with other similar models. We also discuss the various challenges of safety evidence traceability and its application.

5.1 Comparison with Other Models

An important difference between SafeTIM and other evidence models (e.g., [24]) is the explicit distinction between artefacts and their use as evidence. In our notion, a piece of evidence cannot exist on its own. An artefact only represents information used, modified, or produced in some activity. An artefact can be used as evidence when associated to a claim. Furthermore, an artefact can be used as evidence for several claims. As a result, emergent evidence properties arise that do not exist in an artefact per se. Such properties depend on a claim. For example, an artefact can

support some claims and challenge others. The need of defining new concepts in a conceptual model in such cases has been acknowledged in the literature (e.g., [30]).

When compared to the models reviewed in Section 2.2, SafeTIM can be regarded as a combination of some models. For example, SafeTIM includes process-related and artefact-related information as in [25], and evidence-specific information as in [26]. On the other hand, some models (e.g., [4][25]) correspond to instances of SafeTIM. This is logical given the fact that these models are specific to some projects or safety standards and SafeTIM provides a more abstract picture. In this sense, we have benefited from the past work while trying to mitigate and address possible gaps and limitations. One of such limitation, and as explained above, is the need for differentiating artefacts and pieces of evidence in the model.

One aspect that must be noted in SafeTIM is that it only includes direct relationships to and from safety evidence (i.e., to and from the *Artefact* and *Piece of Evidence* classes). More relationships can be maintained to and from the other classes, and thus indirect relationships with evidence can exist. For example, an activity in a project can correspond to the materialisation of a reference activity of a safety standard. Likewise, relationships can be established between *Activity* and *Technique* in order to specify the techniques used to perform some activity. In addition, more classes can be included for modelling the possible attributes of an *Artefact* (e.g., the result of the execution of a test case, which could be passed or failed) to extend SafeTIM.

Although SafeTIM tries to provide a global picture, we understand and acknowledge that it cannot be regarded as a fully finished model. Firstly, and as we have mentioned, it only deals with the direct relationships to and from evidence. Secondly, the model will be integrated in a common certification framework (Section 2.1). This framework will consist of more concepts and relationships. Thirdly, the model has only been validated in a static way [35]. We plan to conduct case studies to analyse how practitioners can benefit from using SafeTIM. Finally, tool support must be developed to facilitate the adoption of SafeTIM in the industry.

Last but not least, and as acknowledged by several authors (e.g., [4][36][37]), defining a traceability information model at the earliest is essential so that traceability activities succeed in industry. Therefore, we believe that SafeTIM can definitely enable and improve safety evidence traceability practice.

5.2 Challenges for Safety Evidence Traceability

We regard the following list as the major challenges for safety evidence traceability in practice nowadays. Some of these challenges are specific to safety evidence, while others are generic challenges to traceability that has significant effect on safety-critical systems.

Vast Amount of Artefacts and Evidence to Trace. Management of vast amounts of data has always been a challenge for information systems [30], but it becomes even more demanding in the safety-critical domain due to strict regulatory compliance and the vast amount of evidence to create, maintain and trace. For example, we identified a set of 49 basic, generic types of safety evidence from the literature [1], which can correspond to over 100 types for some standards (e.g., [31]). In addition to the

challenges inherent to traceability, practitioners can have problems to ensure the consistency of evidence traces. Guidance and tool support are necessary.

Artefacts and Evidence Can be Located in Many Different Locations. Building a critical-system in parts simultaneously in different locations around the world can cause problems in traceability since artefacts used as evidence are in locations different to where the final certification documentation (e.g., a safety case) is developed. This causes problems, such as the coordination of work among distributed development teams and difficulties to ensure that the results are consistent and will not pose any certification risk.

Artefacts and Evidence are Created with and Stored in Different Tools. System suppliers usually have a tool-chain for development, and seamless integration of these tools for safety evidence collection can be difficult. Evidence combination can also be hindered because of the heterogeneity in the formats of the artefacts [24].

Confidence in the Traces Maintained. One of the main challenges that both system suppliers and certifiers face is in gaining confidence in the traces maintained. Providing traces to and from safety evidence are far from enough, as practitioners must aim to be sure that the traces presented are consistent and correct [8].

High Effort and Cost. Although better traceability practices can reduce development effort and costs [9], reality is that it is still a time-consuming activity. As a result, practitioners can end up only dealing with a limited set of traces, usually those mandatory for compliance. However, this might pose certification risks later, or make change management very expensive. Again, adequate guidance and tool support are very important to face this challenge.

Need for Purpose, Value-Based Traceability. In relation to the previous challenge, it is essential that the need for and purpose of safety evidence traceability is clear to those involved in the activity [8]. Otherwise, traceability might not be managed as well as it should be, or its importance might be underestimated. Practitioners must define and be aware of the value of tracing beyond the scope of a single project. For example, adequate safety evidence traceability can facilitate system reuse and change impact analysis in the future, and thus reduce costs.

Some of the above challenges such as the *vast amount of artefacts and evidence to trace, artefacts and evidence located in many different locations*, and *artefacts are created with and stored in different tools* can be tackled by employing a good traceability strategy such as the one proposed in this paper.

6 Conclusion

This paper has presented an analysis of safety evidence traceability based on our knowledge of the state of the art and practice on safety evidence management. The paper presents what we consider as the major motivations that drive the need for evidence traceability. The paper also identifies the traces that need to be created and maintained between safety evidence information items and between evidence and other assurance assets such as claims. As a result of this analysis, we have proposed SafeTIM, a traceability information model for safety evidence.

SafeTIM provides the set of fundamental concepts and relationships necessary to enact evidence traceability in real industrial settings. In addition to making a clear distinction between the artefacts managed during system lifecycle and their use as evidence for a claim, SafeTIM tries to provide a global picture of evidence traceability. We have validated the model with documentation from three different real safety assurance and certification projects. The validation showed that all the classes and relationships of SafeTIM were present in the documentation. In some cases, the presence of the classes and relationships was implicit.

The paper has also compared SafeTIM with other related models and presented what we regard as the major challenges for evidence traceability. In general, we consider that new guidance and tool support can significantly facilitate evidence traceability in industry.

As future work, we plan to extend SafeTIM within the context of the common certification framework to be developed in OPENCOSS, and further validate and evaluate the model in industrial case studies. We also aim to find solutions to some of the challenges presented in the paper.

Acknowledgments. The research leading to this paper has received funding from the FP7 programme under the grant agreement n° 289011 (OPENCOSS) and from the Research Council of Norway under the project Certus-SFI. We also thank the OPENCOSS partners and the colleagues who have provided input and feedback.

References

1. Nair, S., et al.: Classification, Structuring, and Assessment of Evidence For Safety: A Systematic Literature Review. In: ICST, pp. 94–103 (2013)
2. IEEE: IEEE Standard Glossary of Software Engineering Terminology, Std. 610.12-1990
3. Alexander, R., Kelly, T., Gorry, B.: Safety Lifecycle Activities for Autonomous Systems Development. In: SEAS/TR/2009/2 (2009)
4. Cleland-Huang, J., Heimdahl, M., Huffman Hayes, J., Lutz, R., Maeder, P.: Trace queries for safety requirements in high assurance systems. In: Regnell, B., Damian, D. (eds.) REFSQ 2011. LNCS, vol. 7195, pp. 179–193. Springer, Heidelberg (2012)
5. Habli, I., Kelly, T.: A model-driven approach to assuring process reliability. In: ISSRE 2008, pp. 7–16 (2008)
6. Nair, S., et al.: The State of the Practice on Evidence Management for Compliance with Safety Standards. Simula Research Lab. Technical Report (2013)
7. de la Vara, J.L., Panesar-Walawege, R.K.: SafetyMet: A metamodel for safety standards. In: Moreira, A., Schätz, B., Gray, J., Vallecillo, A., Clarke, P. (eds.) MODELS 2013. LNCS, vol. 8107, pp. 69–86. Springer, Heidelberg (2013)
8. Cleland-Huang, J., et al.: Software and systems traceability. Springer-Verlag New York Incorporated (2012)
9. Nair, S., De la Vara, J.L., Sen, S.: A Review of Traceability Research at the Requirements Engineering Conference. In: RE (2013)
10. Torkar, R., et al.: Requirements traceability: a systematic literature review and industry case study. IJSEKE 22(3), 1–49 (2012)
11. Regan, G., et al.: Traceability-Why do it? In: SPICE 2012, pp. 161–172 (2012)
12. Regan, G., et al.: The Barriers to Traceability and their Potential Solutions: Towards a Reference Framework. In: SEAA 2012, pp. 319–322 (2012)

13. Gotel, O., Cleland-Huang, J., Hayes, H., Zisman, A., Egyed, A., Grunbacher, P., Antoniol, G.: The quest for Ubiquity: A roadmap for software and systems traceability research. In: 2012 20th IEEE International Requirements Engineering Conference (RE), pp. 71–80. IEEE (2012)
14. Spanoudakis, G., Zisman, A.: Software traceability: a roadmap. Handbook of Software Engineering and Knowledge Engineering 3, 395–428 (2005)
15. Pohl, K.: Requirements engineering: fundamentals, principles, and techniques. Springer Publishing Company, Incorporated (2010)
16. Lee, J.S., et al.: Means-ends and whole-part traceability analysis of safety requirements. Journal of Systems and Software 83, 1612–1621 (2010)
17. Mason, P.A.J., Saeed, A., Riddle, S.: On the role of traceability for standards compliance: Tracking requirements to code. In: Anderson, S., Felici, M., Littlewood, B. (eds.) SAFECOMP 2003. LNCS, vol. 2788, pp. 303–316. Springer, Heidelberg (2003)
18. Ridderhof, W., Gross, H.-G., Doerr, H.: Establishing evidence for safety cases in automotive systems–A case study. In: Saglietti, F., Oster, N. (eds.) SAFECOMP 2007. LNCS, vol. 4680, pp. 1–13. Springer, Heidelberg (2007)
19. Nejati, S., et al.: A SysML-based approach to traceability management and design slicing in support of safety certification: Framework, tool support, and case studies. Information and Software Technology 54, 569–590 (2012)
20. Katta, V., Stalhane, T.: A conceptual model of traceability for safety systems. In: CSDM-Poster Presentation (2010)
21. Zoughbi, G., Briand, L., Labiche, Y.: Modeling safety and airworthiness (RTCA DO-178B) information: conceptual model and UML profile. Software & Systems Modeling 10, 337–367 (2011)
22. Born, M., et al.: Application of ISO DIS 26262 in practice. In: CARS 2010, pp. 3–6 (2010)
23. Graydon, P., Habli, I., Hawkins, R., Kelly, T., Knight, J.: Arguing Conformance. IEEE Software 29, 50–57 (2012)
24. OMG: Structured Assurance Case Metamodel (SACM) (2013)
25. Panesar-Walawege, R.K., et al.: Supporting the Verification of Compliance to Safety Standards via Model-Driven Engineering: Approach, Tool-Support and Empirical Validation. Information and Software Technology 55(5), 836–864 (2012)
26. Sun, L., Kelly, T.: Elaborating the Concept of Evidence in Safety Cases. In: SCSC 2013 (2013)
27. RTCA: DO-178C - Software Considerations in Airborne Systems and Equipment (2012)
28. De la Vara, J.L., et al.: Towards a model-based evolutionary chain of evidence for compliance with safety standards. In: SAFECOMP 2012 Workshops, pp. 64–78 (2012)
29. Oxford Dictionaries (online), `http://oxforddictionaries.com`
30. Olivé, A.: Conceptual Modeling of Information Systems. Springer (2007)
31. ISO: International Standard Road vehicles - Functional safety - ISO/DIS 26262 (2011)
32. CENELEC: Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems - EN 50128 (2011)
33. Leveson, N.: The Use of Safety Cases in Certification and Regulation. Journal of System Safety 47 (2011)
34. OPENCOSS: D1.2 – Use case description and business impact (2012)
35. Gorschek, T., et al.: A model for technology transfer in practice. IEEE Software 23, 88–95 (2006)
36. Gotel, O., et al.: The quest for Ubiquity: A roadmap for software and systems traceability research. In: RE 2012, pp. 71–80 (2012)
37. Mäder, P., Jones, P., Zhang, Y., Cleland-Huang, J.: Strategic Traceability for Safety-Critical Projects. IEEE Software 30(3), 58–66 (2013)