Electronic Supplementary Material (ESM)

Automated Traceability Compliance Assessment for Safety-Critical Software

Patrick Rempel, Mario Janke, Martin Rabe and Patrick Mäder

Technische Universität Ilmenau, Ilmenau, Germany
e-mail: patrick.rempel@tu-ilmenau.de, patrick.maeder@tu-ilmenau.de

Contents

A.1 Prototype

A.2 Questionnaire used for the expert study with certifiers and safety-critical project participants

A.3 Anonymized survey results

A.1 Prototype

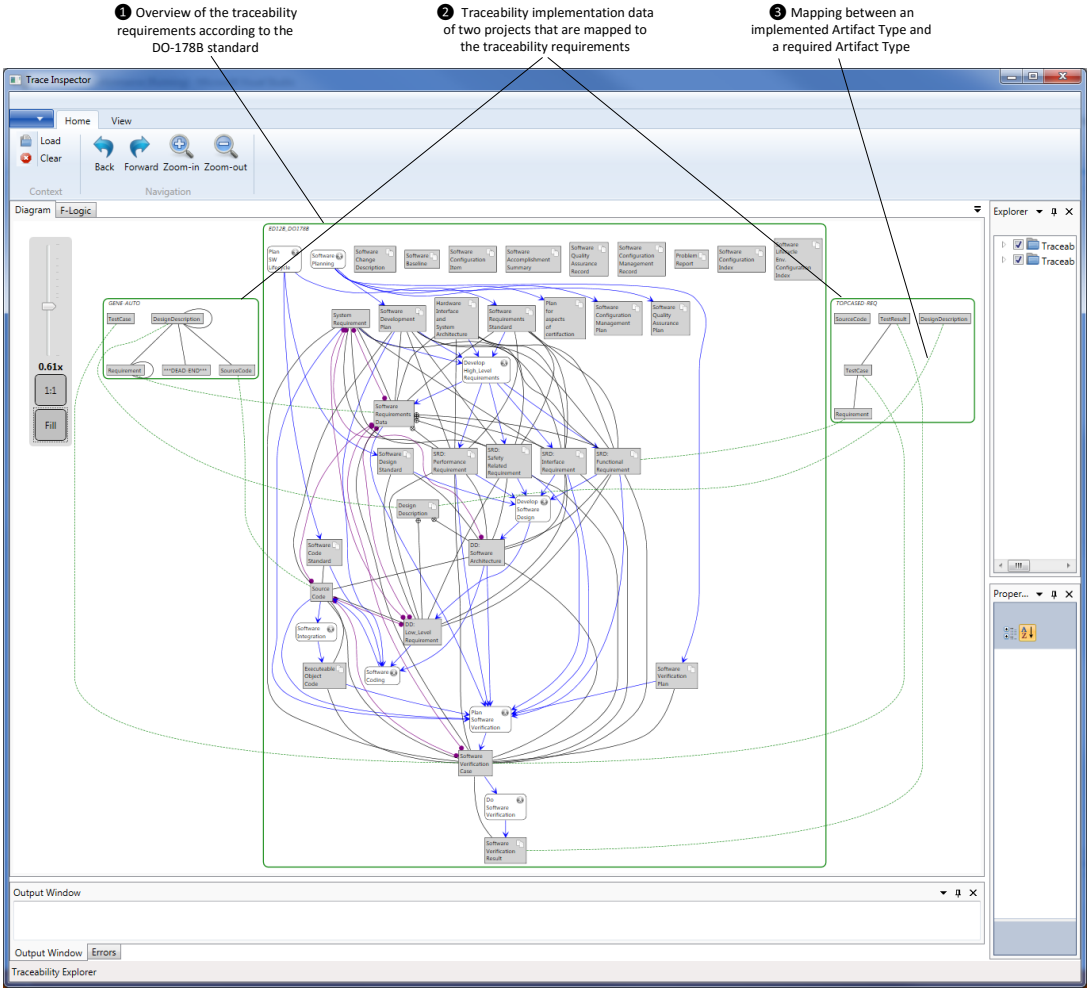


Figure A.1: Screenshot of the traceability browser that visualizes the traceability needs derived from the DO-178 guideline and the artifact types of two projects at zoom level zero

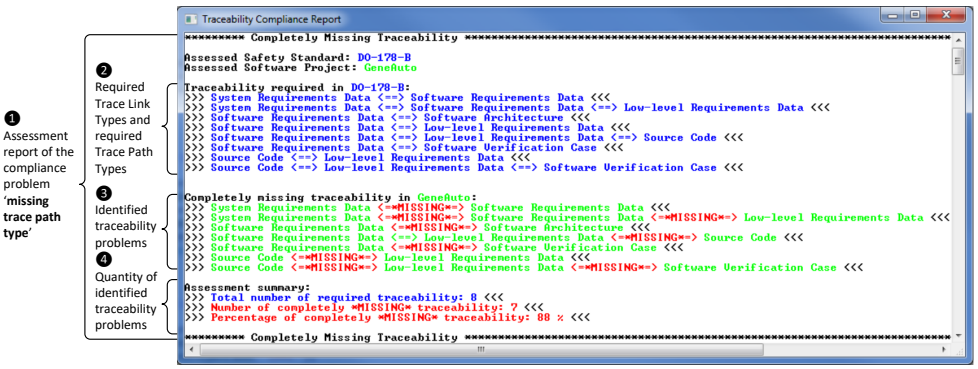


Figure A.2: Example of an assessment report for traceability problem: missing trace path type

A.2 Questionnaire used for the expert study with certifiers and safety-critical project participants

Questionnaire

In this questionnaire we ask for your opinion on a technique we developed to automatically assess the traceability compliance of software development data with functional safety standards. The questionnaire is structured as follows:

1. We provide an **Introduction** to relevant terms (e.g. traceability, functional safety, safety standards) and explain our traceability compliance assessment technique.
2. We ask **Preliminary Questions** about your software engineering background.
3. We ask for **Your Opinion** on our traceability compliance assessment technique based on your practical experience.

Additional facts:

- Completing this questionnaire will take approximately **30 minutes**.
- Please answer **all questions** that are marked with ✎.
- This questionnaire is **anonymous** and the results are used for research only.
- Target audience: people who are/were concerned (in)directly with the development of software-based systems that need to achieve functional safety.
- All participants of this survey will receive a **detailed report** on the results and are welcome to run the compliance assessment on their own software projects data.

Contact informations:

✉ Technische Universität Ilmenau
Patrick Rempel
Software Systems / Process Informatics
Helmholtzplatz 5
98693 Ilmenau

@ patrick.rempel@tu-ilmenau.de

☎ +49 3677 / 69-4182

Introduction

Many **software safety standards**[1] prescribe **traceability**[2] to demonstrate that a rigorous software development process has been followed. Traceability *supports* the achievement of **Functional Safety**[3] of software-based systems, because it ensures that:

- all **potential hazards, risks and regulations** are *addressed* by requirements,
- all **requirements** are *implemented* and *verified*,
- no **unintended functionality** is *implemented* but only required functionality.

Increasingly, certification to software safety standards is desired by end-users and encouraged by regulatory authorities to minimize the risk of use.

It is the **certifier's** responsibility during certification to *check* whether or not a developed **software product** *complies* with a **standard**. In terms of traceability, the **certifier** needs to check whether or not the software development data (e.g. requirements, design document, source code, test cases) are traceable as prescribed by a standard.

Software engineers, developing safety-critical software, have the responsibility to *develop* **software products** that *comply* with a **standard**. Thus, **software engineers** need the ensure that all software development data (e.g. requirements, design, source code, test cases) are traceable as prescribed by a standard.

We have developed an **assessment tool** that *automatically checks* **traceability compliance** of software development data to safety standards. The tool's main goal is to *support* **software engineers** and **certifiers**.

The traceability compliance assessment tool works as follows:

- We defined **5 problem classes**. We *claim* that the existence of such problems in software development data *indicate* the **non-compliance** of traceability.
- The tool *searches* for **problem instances** within the software development data.
- The tool *generates* **assessment reports** for every problem class.

In this questionnaire, we provide **illustrating examples**, which are *based* on the **DO-178B** standard for software within aircrafts[4] and on the industrial development project **Gene-Auto**, which has the explicit project goal to comply with the DO-178B standard.

[1] A **software safety standard** specifies requirements for software development that need to be satisfied to ensure that the developed software is safe for use.
[2] **Traceability** is the ability to trace the origin, the evolution, and the result of any software development data (e.g. requirements, design, source code), even after the development has been completed.
[3] The objective of **Functional Safety** is freedom from unacceptable risk of physical injury or of damage to the health of people either directly or indirectly through damage to property or to the environment.
[4] **DO-178B**: Software Considerations in Airborne Systems and Equipment Certification.

Preliminary Questions

Please rate your **practical experience** in software development projects.

☐ years (Please round to full years)

What is your **primary role** in software engineering? (Please select one)

◯ Developer	◯ Tester	◯ Consultant	◯ Safety Engineer
◯ Manager	◯ Analyst	◯ Administrator	◯ Certification Engineer
◯ Architect	◯ Auditor	◯ Trainer	◯ ☐

Are / were you concerned with **additional role(s)** in software engineering? (Please select all that apply)

☐ Developer	☐ Tester	☐ Consultant	☐ Safety Engineer
☐ Manager	☐ Analyst	☐ Administrator	☐ Certification Engineer
☐ Architect	☐ Auditor	☐ Trainer	☐ ☐

In which **domain(s)** are/were you working? (Please select all that apply)

☐ Aviation	☐ Automotive	☐ Energy	☐ Railway
☐ Space	☐ Medical	☐ Agriculture	☐ Industrial Automation
☐ Military	☐ Maritime	☐ Mining	☐ ☐

Are you **familiar** with **functional safety** of software-based systems? (Please select one)

Not familiar	I know the objectives	$\leq$ 1 year experience	$\geq$ 2 years experience	Expert
◯	◯	◯	◯	◯

Have you **participated** in a project that was aiming to ensure functional safety?

◯ Yes ◯ No (Please select one)

Have you **participated** in a project that was certified for functional safety?

◯ Yes ◯ No (Please select one)

Have you **certified** the functional safety of a software project?

◯ Yes ◯ No (Please select one)

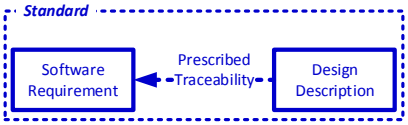
Which of the following functional safety standards are/were relevant for your current or previous work? (Please select all that apply)

☐ IEC 61508	☐ IEC 61513	☐ DO-178 B/C	☐ IEC 62304
☐ ISO 26262	☐ EN 50128	☐ ISO 25119	☐ ☐

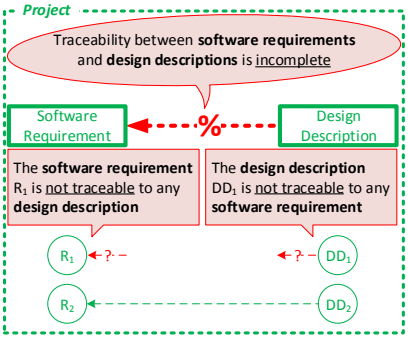
Your Opinion - 1st Problem Class

Traceability between two types of software development data is ***incomplete***.

Illustrating example:



The **DO-178B** standard prescribes: "**Desgin descriptions** developed during the design process should be traceable to **software requirements**".



Situation within the project: **Software requirements** and **design descriptions** are available. Traceability between **software requirements** and **design descriptions** is available. Though, the traceability is *incomplete*, because the software requirement R_1 is not traceable to any design description and the design description DD_1 is not traceable to any software requirement.

We claim that incomplete traceability indicates ***non-compliance*** *of traceability with a standard.*

What is **your opinion** based on your practical experience? (Please select one)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

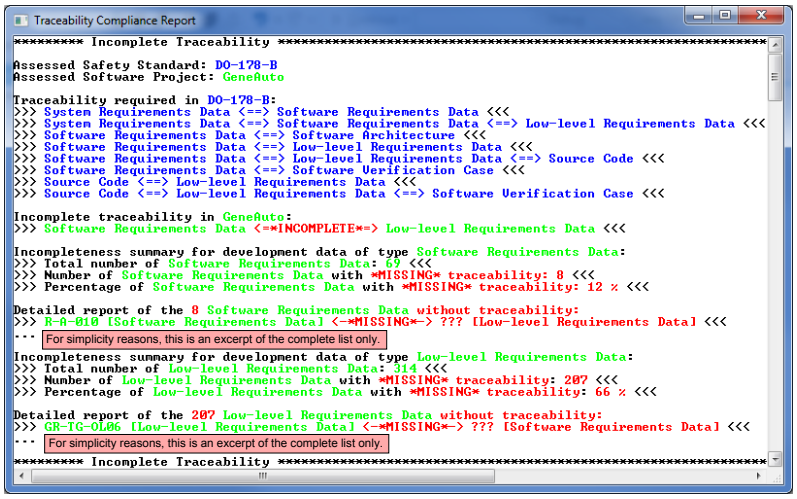
We claim that incomplete traceability indicates ***safety risks****.*

What is **your opinion** based on your practical experience? (Please select one)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

Exemplary assessment report for the 1st problem class:



Is the reported information helpful for a **certifier** to check the compliance of **GeneAuto's** traceability with the **DO-178B** standard?
(Please select one answer)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

Is the reported information helpful for a **project participant** to ensure the compliance of **GeneAuto's** traceability with the **DO-178B** standard?
(Please select one answer)

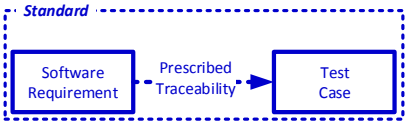
Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

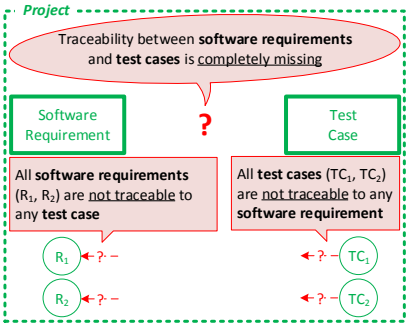
Your Opinion - 2nd Problem Class

Traceability between two types of software development data is ***completely missing***.

Illustrating example:



The **DO-178B** standard prescribes: "The verification process provides traceability between **software requirements** and **test cases**".



Situation within the project: **Software requirements** and **test cases** are available. Traceability between **software requirements** and **test cases** is *completely missing*.

We claim that missing traceability indicates ***non-compliance*** *of traceability with a standard.*

What is **your opinion** based on your practical experience? (Please select one)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

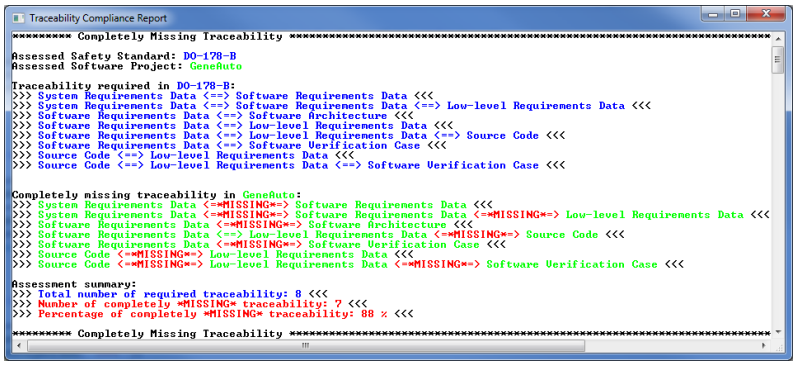
We claim that missing traceability indicates ***safety risks***.

What is **your opinion** based on your practical experience? (Please select one)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

Exemplary assessment report for the 2nd problem class:



Is the reported information helpful for a **certifier** to check the compliance of **GeneAuto's** traceability with the **DO-178B** standard?
(Please select one answer)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

Is the reported information helpful for a **project participant** to ensure the compliance of **GeneAuto's** traceability with the **DO-178B** standard?
(Please select one answer)

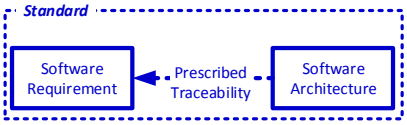
Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

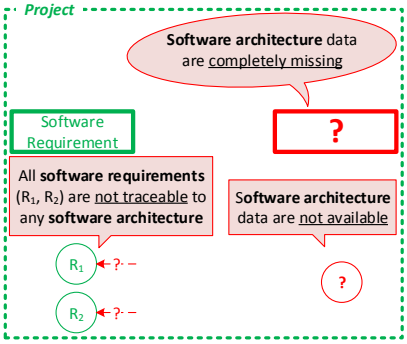
Your Opinion - 3rd Problem Class

A **type of software development data** for which traceability is prescribed is ***completely missing***.

Illustrating example:



The **DO-178B** standard prescribes: "**Software architecture**, developed during the design process, should be *traceable* to **software requirements**".



Situation within the project: **Software requirements** data are available, **software architecture** data are completely *missing*. This implies that prescribed traceability can not be created between **software requirements** data and the missing **software architecture** data.

We claim that missing software development data, for which traceability is prescribed, indicate ***non-compliance*** *of traceability with a standard.*
What is **your opinion** based on your practical experience? (Please select one)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

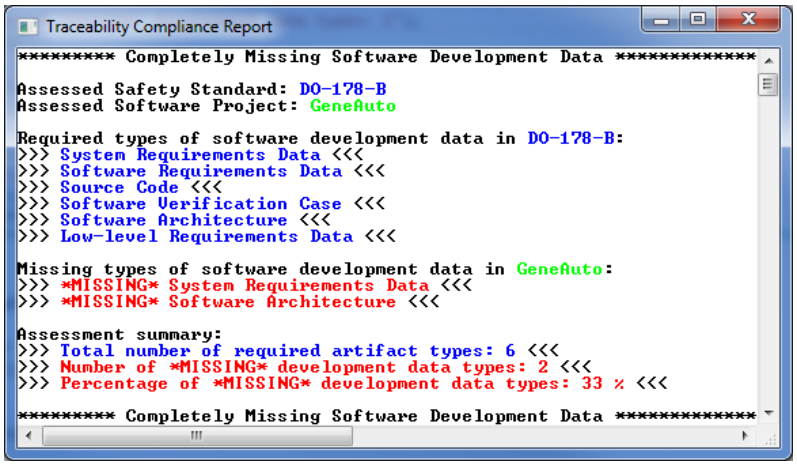
Can you briefly explain why you agree or disagree?

We claim that missing software development data, for which traceability is prescribed, indicate ***safety risks***.
What is **your opinion** based on your practical experience? (Please select one)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

Exemplary assessment report for the 3rd problem class:



Is the reported information helpful for a **certifier** to check the compliance of **GeneAuto's** traceability with the **DO-178B** standard?
(Please select one answer)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

Is the reported information helpful for a **project participant** to ensure the compliance of **GeneAuto's** traceability with the **DO-178B** standard?
(Please select one answer)

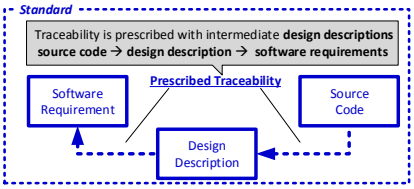
Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

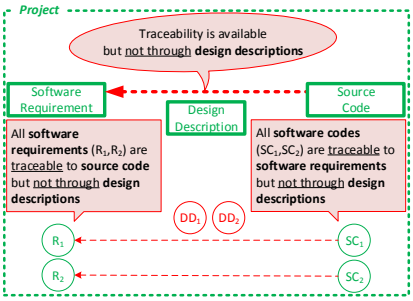
Your Opinion - 4^{th} Problem Class

Traceability is available but ***deviates*** from the prescription.

Illustrating example:



The **DO-178B** standard prescribes: "Traceability between the **source code** and **software requirements** throughout **design descriptions** should be provided to give visibility to the design decision made during the design process and to allow verification of the complete implementation of the software requirements."



Situation within the project: **Software requirements**, **design descriptions**, and **source code** are available. Traceability between **software requirements** and **source code** is available. Traceability *deviates* from the standard because it does not include **design descriptions**. Thus, it cannot be used to give visibility to the design decision.

We claim that deviating traceability indicates ***non-compliance*** *with a standard.*
What is **your opinion** based on your practical experience? (Please select one)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

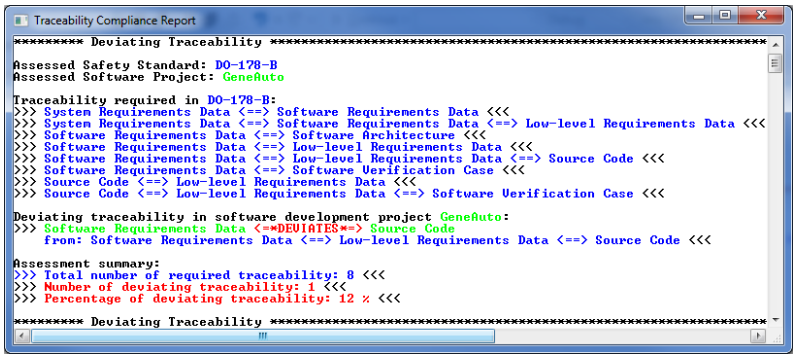
Can you briefly explain why you agree or disagree?

We claim that deviating traceability indicates ***safety risks****.*
What is **your opinion** based on your practical experience? (Please select one)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

Exemplary assessment report for the 4^{th} problem class:



Is the reported information helpful for a **certifier** to check the compliance of **GeneAuto's** traceability with the **DO-178B** standard?
(Please select one answer)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

Is the reported information helpful for a **project participant** to ensure the compliance of **GeneAuto's** traceability with the **DO-178B** standard?
(Please select one answer)

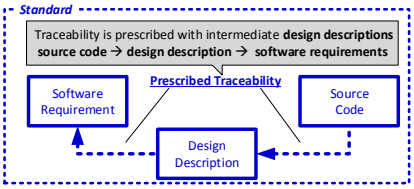
Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

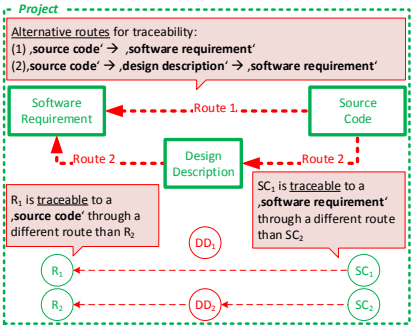
Your Opinion - 5th Problem Class

Traceability is available but with ***alternative routes***.

Illustrating example:



The **DO-178B** standard prescribes: "Traceability between the **source code** and **software requirements** throughout **design descriptions** should be provided to give visibility to the design decision made during the design process and to allow verification of the complete implementation of the software requirements."



Situation within the project: **Software requirements**, **design descriptions**, and **source code** are available. Traceability between **software requirements** and **source code** is available. Though, the project provides *ambiguous* traceability: some **source codes** are directly traced to **software requirements**, other **source codes** are traced through **design descriptions** to **software requirements**.

We claim that ambiguous traceability indicates ***non-compliance*** *of traceability.*
What is **your opinion** based on your practical experience? (Please select one)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

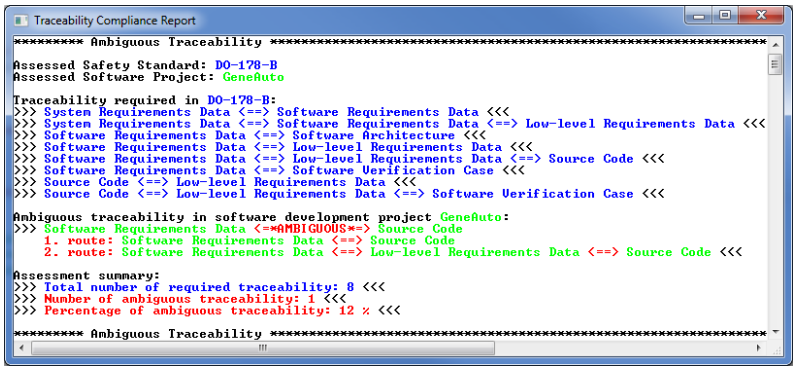
Can you briefly explain why you agree or disagree?

We claim that ambiguous traceability indicates ***safety risks***.
What is **your opinion** based on your practical experience? (Please select one)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

Exemplary assessment report for the 5^{th} problem class:



Is the reported information helpful for a **certifier** to check the compliance of **GeneAuto's** traceability with the **DO-178B** standard?
(Please select one answer)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

Is the reported information helpful for a **project participant** to ensure the compliance of **GeneAuto's** traceability with the **DO-178B** standard?
(Please select one answer)

Strongly Agree	Agree	Disagree	Strongly Disagree	Don't know
○	○	○	○	○

Can you briefly explain why you agree or disagree?

A.3 Anonymized quantitative survey results

Variable	**Sub-variable**	**Type**	**Subjects' responses**																	$\sum$
Work experience		years	15	30	20	10	15	4	20	6	13	7	15	12	45	18	10	10	10	
Primary role	developer	yes/no	0	0	0	1	0	1	0	1	1	0	0	0	0	0	1	0	0	5
Primary role	manager	yes/no	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	4
Primary role	architect	yes/no	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
Primary role	tester	yes/no	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Primary role	analyst	yes/no	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Primary role	auditor	yes/no	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Primary role	consultant	yes/no	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	3
Primary role	administrator	yes/no	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Primary role	trainer	yes/no	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Primary role	safety engineer	yes/no	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	2
Primary role	certification engineer	yes/no	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Secondary role	developer	yes/no	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	4
Secondary role	manager	yes/no	0	0	0	0	0	0	1	1	0	0	1	0	1	1	0	0	0	5
Secondary role	architect	yes/no	1	0	0	1	0	1	0	1	1	1	0	1	0	0	0	0	0	7
Secondary role	tester	yes/no	0	0	0	1	1	1	1	1	1	1	0	0	0	0	1	1	0	9
Secondary role	analyst	yes/no	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	1	0	5
Secondary role	auditor	yes/no	0	1	0	0	1	0	1	0	0	0	0	1	1	1	0	1	0	7
Secondary role	consultant	yes/no	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	3
Secondary role	administrator	yes/no	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Secondary role	trainer	yes/no	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	0	4
Secondary role	safety engineer	yes/no	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	1	4
Secondary role	certification engineer	yes/no	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	3
Domain	aviation	yes/no	0	1	0	1	1	1	0	0	1	0	0	1	1	1	0	1	0	9
Domain	space	yes/no	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	2
Domain	military	yes/no	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Domain	automotive	yes/no	1	1	1	0	0	0	0	0	1	0	1	0	0	1	1	0	0	7
Domain	medical	yes/no	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	2
Domain	maritime	yes/no	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Domain	energy	yes/no	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Domain	agriculture	yes/no	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1
Domain	mining	yes/no	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Domain	railway	yes/no	0	0	0	0	0	0	1	0	0	0	1	1	0	0	0	1	1	5
Domain	industrial automation	yes/no	1	1	0	0	0	0	1	0	1	0	0	0	1	0	1	0	1	7
Safety expertise	not familiar	yes/no	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Safety expertise	know objectives	yes/no	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	2
Safety expertise	1 year	yes/no	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Safety expertise	$\geq$ 2 year	yes/no	1	0	0	1	0	0	1	1	1	0	1	0	0	1	1	0	0	8
Safety expertise	expert	yes/no	0	1	1	0	1	0	0	0	0	1	0	1	1	0	0	1	0	7
Experience	Member of a safety project	yes/no	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	16
Experience	Member of a certified project	yes/no	0	1	0	1	1	1	1	0	0	1	0	1	1	1	1	1	0	11
Experience	Certified a project	yes/no	0	1	1	0	0	0	0	1	0	0	0	1	1	0	0	1	0	6
Guideline	IEC 61508	yes/no	1	1	0	1	0	0	1	1	0	1	0	0	1	0	1	0	1	9
Guideline	ISO 26262	yes/no	0	0	1	0	0	0	0	0	1	0	1	0	0	0	1	0	1	5
Guideline	IEC 61513	yes/no	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Guideline	EN 50128	yes/no	0	0	0	0	0	0	1	0	1	0	1	1	0	0	0	0	1	5
Guideline	DO 178	yes/no	0	0	0	1	1	1	0	0	1	0	1	1	1	0	1	1	0	9
Guideline	ISO 25119	yes/no	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
Guideline	IEC 62304	yes/no	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Guideline	IEC 61511	yes/no	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2
Guideline	IEC 62061	yes/no	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Guideline	IEC 50129	yes/no	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1
Guideline	ISO 14121	yes/no	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	2
Guideline	ISO 13849	yes/no	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	2
1^{st} Problem	Traceability compliance	Likert	1	2	-1	2	2	2	2	2	1	2	1	-1	2	2	-1	-1	2	
1^{st} Problem	Safety risks	Likert	-1	2	2	-1	2	2	2	1	1	1	1	2	2	-1	-1	1	2	
1^{st} Problem	Helpfulness certifier	Likert	1	0	2	-2	1	2	2	0	1	1	0	2	2	1	0	-1	2	
1^{st} Problem	Helpfulness project member	Likert	0	0	1	-2	1	2	2	2	1	1	0	1	2	1	1	1	2	
2^{nd} Problem	Traceability compliance	Likert	1	2	2	2	1	2	2	2	2	2	1	2	2	-1	1	2	2	
2^{nd} Problem	Safety risks	Likert	1	2	2	2	1	2	2	1	2	1	1	1	2	1	-1	2	2	
2^{nd} Problem	Helpfulness certifier	Likert	1	0	2	-2	1	1	2	0	2	1	0	1	2	1	0	-1	2	

2^{nd} Problem	Helpfulness project member	Likert	1	0	2	-2	1	1	2	2	2	1	0	1	2	2	1	-1	2	
3^{rd} Problem	Traceability compliance	Likert	1	2	-1	-2	1	2	1	2	1	2	1	1	2	1	2	-1	1	
3^{rd} Problem	Safety risks	Likert	1	2	-1	2	1	0	1	2	1	1	1	-1	1	-1	1	-1	1	
3^{rd} Problem	Helpfulness certifier	Likert	0	0	1	-2	1	2	1	-1	1	1	0	1	1	0	-1	-1	1	
3^{rd} Problem	Helpfulness project member	Likert	0	0	2	-2	1	2	1	-1	1	1	0	1	1	1	-1	-1	1	
4^{th} Problem	Traceability compliance	Likert	-1	2	1	2	1	1	2	1	1	-1	1	0	-2	2	0	-2	2	
4^{th} Problem	Safety risks	Likert	-1	2	-1	1	1	0	1	1	1	-1	1	-1	-2	1	-1	-2	2	
4^{th} Problem	Helpfulness certifier	Likert	1	0	1	-2	1	1	1	-1	1	-1	0	0	0	2	0	-2	2	
4^{th} Problem	Helpfulness project member	Likert	2	0	1	-2	1	1	1	-1	1	-1	0	0	0	2	-1	-2	2	
5^{th} Problem	Traceability compliance	Likert	1	2	-1	2	1	1	1	-1	1	2	1	-1	0	-1	-1	-2	1	
5^{th} Problem	Safety risks	Likert	1	2	1	1	1	-2	1	-1	1	2	1	-1	0	1	0	-2	1	
5^{th} Problem	Helpfulness certifier	Likert	1	0	1	-2	1	1	1	0	1	2	0	0	-2	1	1	-2	1	
5^{th} Problem	Helpfulness project member	Likert	1	0	2	-2	1	1	1	1	1	2	0	0	-2	2	1	-2	1	