Universidade
Federal de
Pernambuco

Integration between Requirements Engineering and Safety Analysis

Jéssyka Vilela

jffv@cin.ufpe.br

Advisor: Jaelson Castro

Co-Advisor: Luiz Eduardo Galvão Martins, Universidade Federal de São Paulo (UNIFESP)

Level: Doctoral

Admission: March/2015

Conclusion: February/2019

04/05/2018

Laboratório de Engenharia
de Requisitos
www.cin.ufpe.br/~ler

Outline

- Overview of research challenges
- Results of a systematic literature review
- References

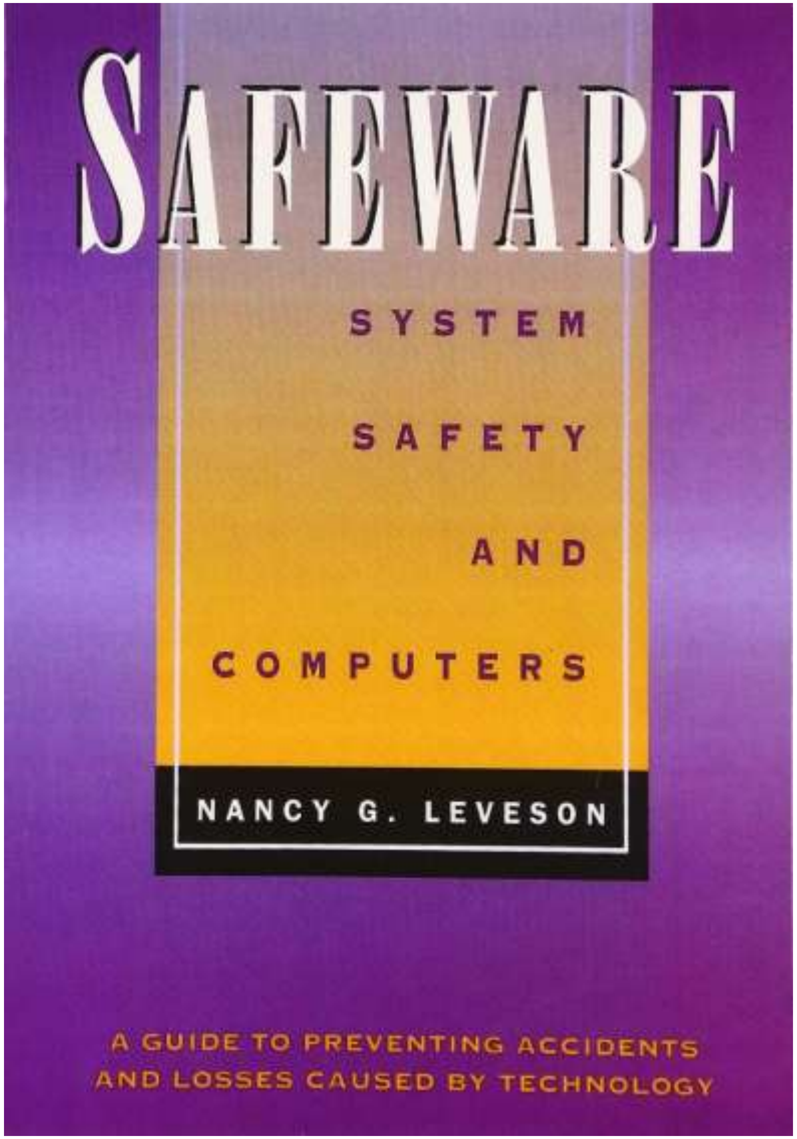
It started in 1986..

- Nancy Leveson brought the notion of “software safety” to the broader computer science community and laid the foundation for a research area rich with challenging problems [1].

- Leveson and others have since then repeatedly pointed out that the phrase “software safety” is somewhat of a misnomer since software by itself is not dangerous.
  - software does not have stored energy that can be released to harm persons, and software is not poisonous or radioactive to harm persons or the environment.

- Safety is a problem in physical systems and software can only contribute to safety (or hazards) in a context.

In 1995, she published [2]..



SAFEWARE

SYSTEM SAFETY AND COMPUTERS

NANCY G. LEVESON

A GUIDE TO PREVENTING ACCIDENTS AND LOSSES CAUSED BY TECHNOLOGY

Then, Robyn Lutz in FOSE (2000)

- **"Software engineering for safety: a roadmap."**
- **Snapshot of six key areas in state-of-the-art software engineering for safety by defining concepts, citing techniques and tools:**

Hazard analysis

Safely requirements specification and analysis

Designing for safety

Testing

Certification and standards

Resources

Then, Robyn Lutz in FOSE (2000)

- Some directions for needed work:

1) Further integration of informal and formal methods.
   - □ Automatic translation of informal notations into formal, Lightweight formal methods.

2) Constraints on safe product families and safe reuse.
   - □ Safety analysis of product families.

3) Testing and evaluation of safety-critical systems.
   - □ Requirements-based testing, Model consistency, Evaluation from multiple sources, Virtual environments.

4) Runtime Monitoring.
   - □ Requirements and architectural analyses are needed for autonomous software.

5) Education.

6) Collaboration with Related Fields.

Matt Heimdahl [4] in FOSE (2007)…

- “Safety and software intensive systems: Challenges old and new."
- Lutz’s challenges are as valid today as they were seven years ago and have been only partially addressed since then.
  - □ Therefore, he did not revisit these challenges.

Matt Heimdahl [4] in FOSE (2007)…

- Matt Heimdahl singled out 4 issues:

1) the nature of safety is continuing to be widely misunderstood and known system safety techniques are not applied;
   - □ education and training of our software engineering professionals.

2) the ability to demonstrate (certify) that safety requirements have been met is inadequate;
   - □ we advocated a move towards evidence-based certification and some notion of safety-cases.

3) the move towards various forms of model-based development with its increased reliance on tools rather than people in the software development process introduces new and poorly understood problems;
   - □ (1) validation of the artifacts (models) forming the basis for tool intensive development, (2) assuring correctness of our automated tools, and (3) investigating the effect of replacing human activities with automated tools.

4) incorrect data of data-driven safety-critical systems could have catastrophic and widespread consequences.
   1) Techniques to assure the validity of the data are needed and we need to closely monitor the convergence of our critical control systems and large information systems.

Sikora et al [5] in REJ (2011)…

- Conducted an industrial study to gain an in-depth understanding of practitioners' needs concerning RE research and method development.

- The study involved qualitative interviews as well as quantitative data collection by means of questionnaires.

- The main results are related to five aspects of RE approaches:
  - □ the use of requirements models
  - □ the support for high system complexity
  - □ quality assurance for requirements
  - □ the transition between RE and architecture design
  - □ the interrelation of RE and safety engineering.

Hatcliff et al. [6] in FOSE (2014) highlighted…

- Certification: Software, Subsystems (Compositional), Tools
- Developing foundational principles
- The nature of criteria in safety
- Requirements
  - □ Requirements Engineering should facilitate the validation needed for assurance by third parties before deployment.
  - □ Many safety-critical systems developed today are built on (or derived from or modifications of) previous versions.
  - □ The processes of system engineering, safety engineering, and software engineering are not well-integrated.
  - □ Domain Specific Languages (DSLs) may be an effective way of achieving this.
    - Paper Specifying Safety Requirements with GORE languages [7].
- Increasing automation in hazard analysis
- Building competence to engineer software for safety critical systems

SLR about communication or integration between RE and safety engineering in SCS [8]

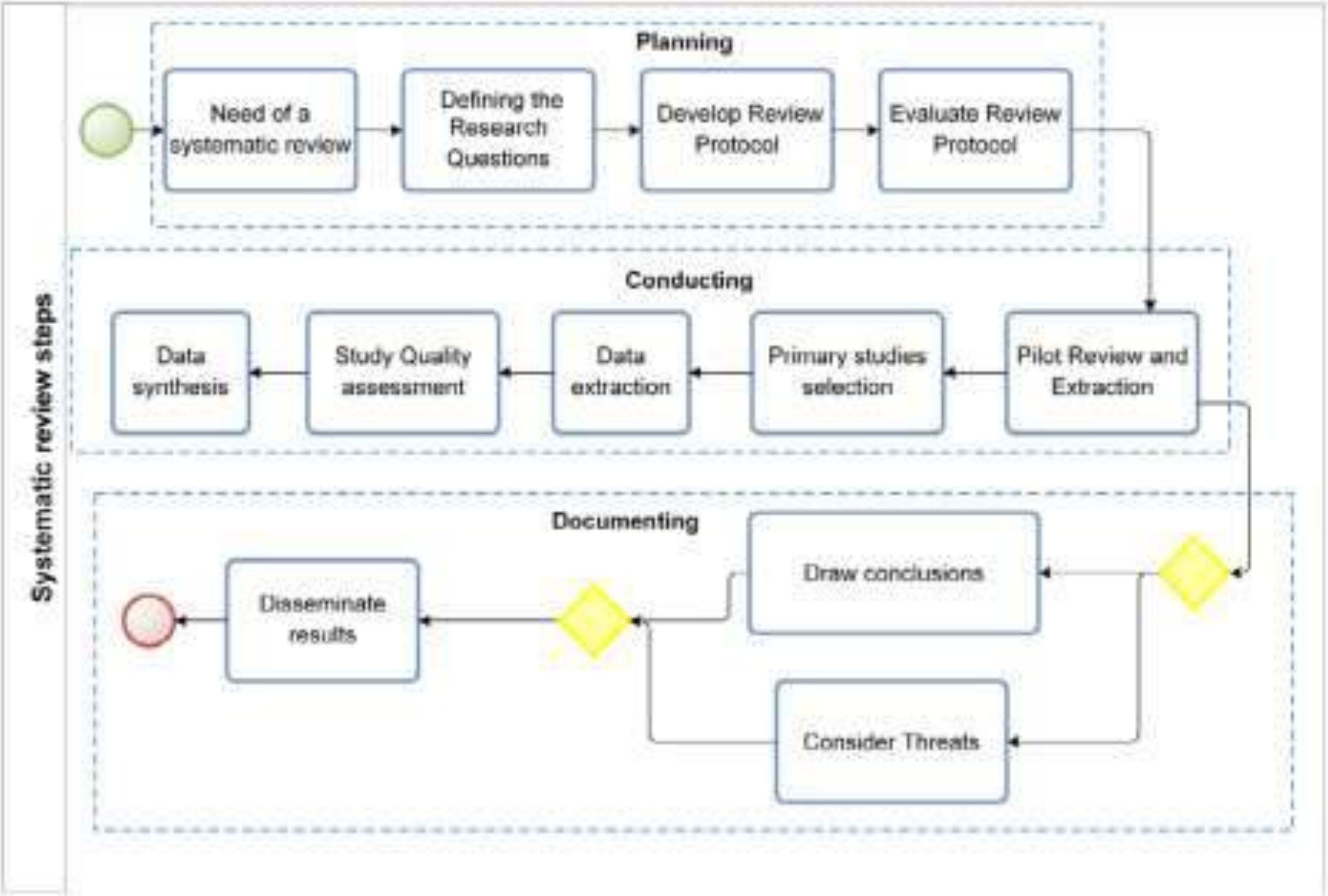


Fig. 1. Systematic review steps adapted from Martins and Gorschek (2016) and Kitchenham and Charters (2007).

Research questions and motivations

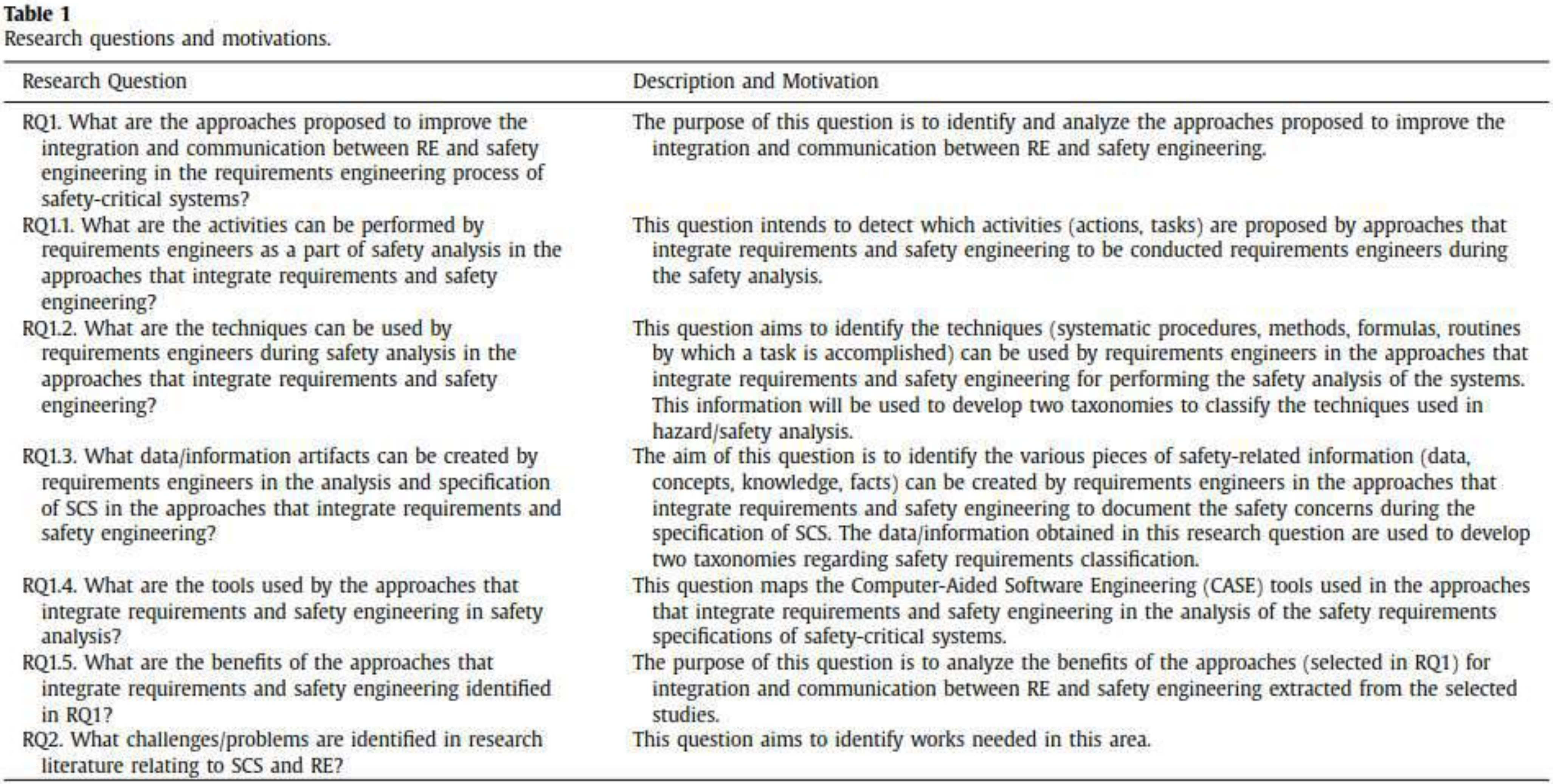


Table 1
Research questions and motivations.

Research Question	Description and Motivation
RQ1. What are the approaches proposed to improve the integration and communication between RE and safety engineering in the requirements engineering process of safety-critical systems?	The purpose of this question is to identify and analyze the approaches proposed to improve the integration and communication between RE and safety engineering.
RQ1.1. What are the activities can be performed by requirements engineers as a part of safety analysis in the approaches that integrate requirements and safety engineering?	This question intends to detect which activities (actions, tasks) are proposed by approaches that integrate requirements and safety engineering to be conducted requirements engineers during the safety analysis.
RQ1.2. What are the techniques can be used by requirements engineers during safety analysis in the approaches that integrate requirements and safety engineering?	This question aims to identify the techniques (systematic procedures, methods, formulas, routines by which a task is accomplished) can be used by requirements engineers in the approaches that integrate requirements and safety engineering for performing the safety analysis of the systems. This information will be used to develop two taxonomies to classify the techniques used in hazard/safety analysis.
RQ1.3. What data/information artifacts can be created by requirements engineers in the analysis and specification of SCS in the approaches that integrate requirements and safety engineering?	The aim of this question is to identify the various pieces of safety-related information (data, concepts, knowledge, facts) can be created by requirements engineers in the approaches that integrate requirements and safety engineering to document the safety concerns during the specification of SCS. The data/information obtained in this research question are used to develop two taxonomies regarding safety requirements classification.
RQ1.4. What are the tools used by the approaches that integrate requirements and safety engineering in safety analysis?	This question maps the Computer-Aided Software Engineering (CASE) tools used in the approaches that integrate requirements and safety engineering in the analysis of the safety requirements specifications of safety-critical systems.
RQ1.5. What are the benefits of the approaches that integrate requirements and safety engineering identified in RQ1?	The purpose of this question is to analyze the benefits of the approaches (selected in RQ1) for integration and communication between RE and safety engineering extracted from the selected studies.
RQ2. What challenges/problems are identified in research literature relating to SCS and RE?	This question aims to identify works needed in this area.

Inclusion/exclusion criteria

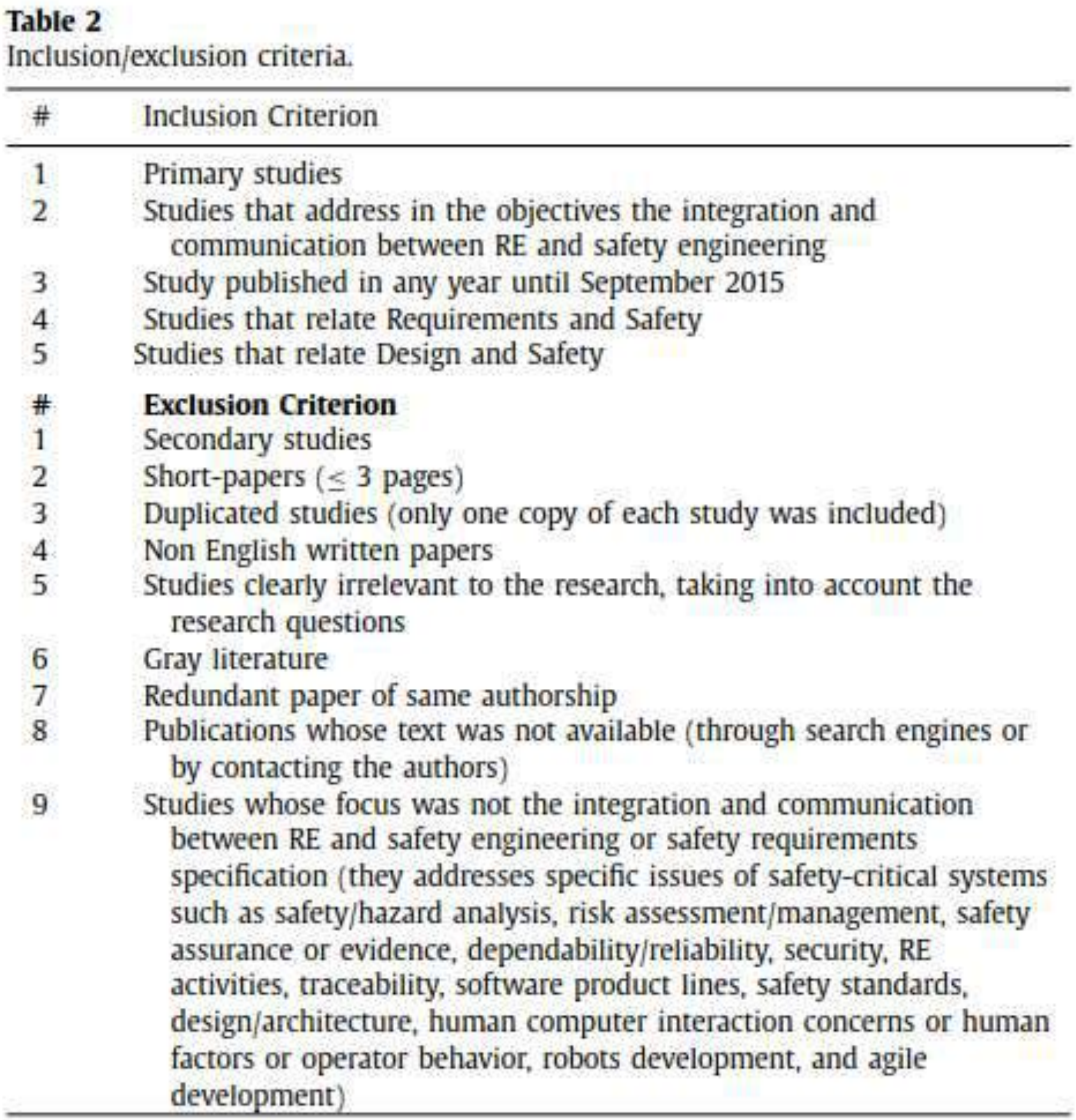


Table 2
Inclusion/exclusion criteria.

#	Inclusion Criterion
1	Primary studies
2	Studies that address in the objectives the integration and communication between RE and safety engineering
3	Study published in any year until September 2015
4	Studies that relate Requirements and Safety
5	Studies that relate Design and Safety
#	**Exclusion Criterion**
1	Secondary studies
2	Short-papers (≤ 3 pages)
3	Duplicated studies (only one copy of each study was included)
4	Non English written papers
5	Studies clearly irrelevant to the research, taking into account the research questions
6	Gray literature
7	Redundant paper of same authorship
8	Publications whose text was not available (through search engines or by contacting the authors)
9	Studies whose focus was not the integration and communication between RE and safety engineering or safety requirements specification (they addresses specific issues of safety-critical systems such as safety/hazard analysis, risk assessment/management, safety assurance or evidence, dependability/reliability, security, RE activities, traceability, software product lines, safety standards, design/architecture, human computer interaction concerns or human factors or operator behavior, robots development, and agile development)

Search string

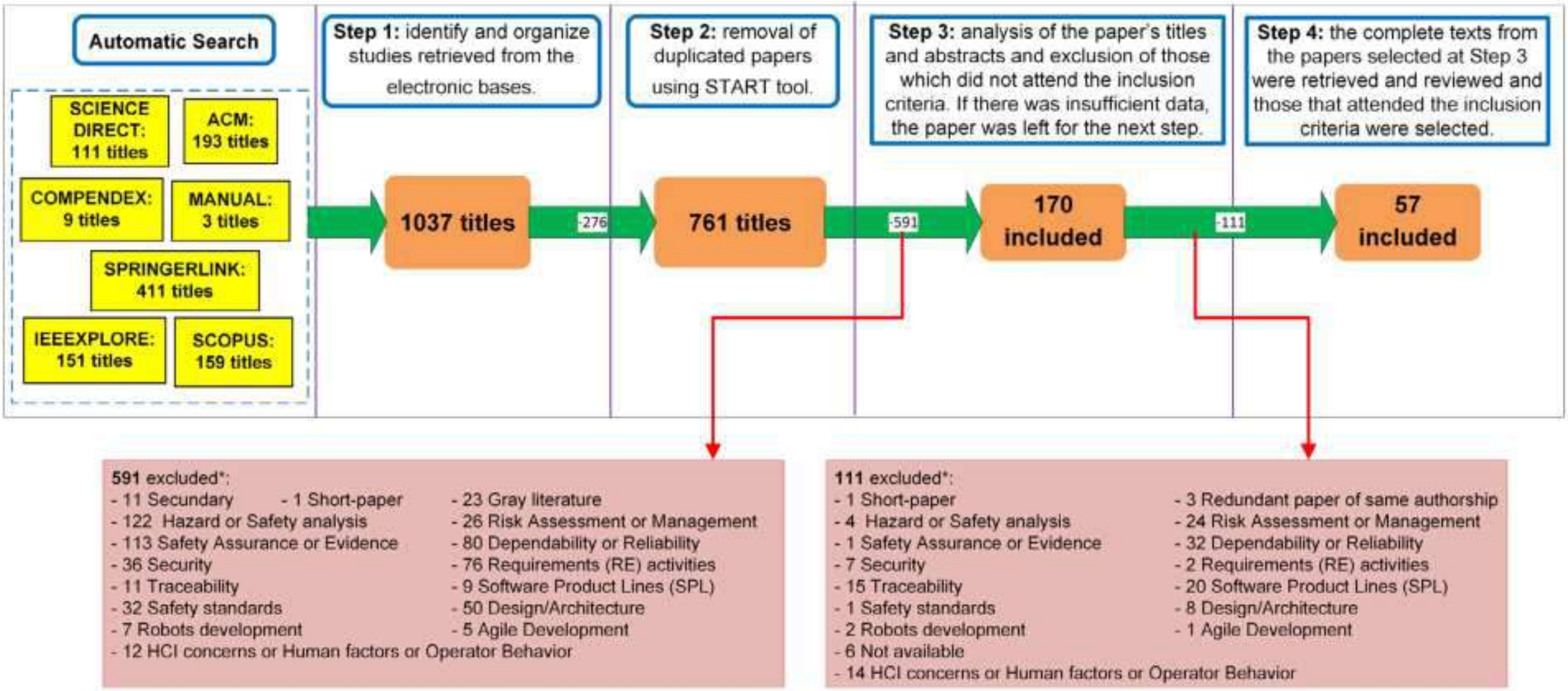
(1) (“safety critical system” OR “safety critical systems” OR “safety-critical system” OR “safety-critical systems”) AND

(2) (“requirements engineering” OR “requirements engineer” OR “requirements team” OR “requirements specification”) AND

(3) (“safety requirements” OR “safety engineering” OR “safety engineer” OR “safety team” OR “safety analysis” OR “safety specification”) AND

(4) (“communication” OR “integration” OR “interaction” OR “collaboration” OR “alignment” OR “understanding” OR “relationship” OR “share” OR “sharing” OR “combination” OR “interrelation” OR “interplay” OR “interdependency”)

Procedure for studies selection



Step 1: identify and organize studies retrieved from the electronic bases.

Step 2: removal of duplicated papers using START tool.

Step 3: analysis of the paper's titles and abstracts and exclusion of those which did not attend the inclusion criteria. If there was insufficient data, the paper was left for the next step.

Step 4: the complete texts from the papers selected at Step 3 were retrieved and reviewed and those that attended the inclusion criteria were selected.

591 excluded*:
- 11 Secundary - 1 Short-paper
- 122 Hazard or Safety analysis
- 113 Safety Assurance or Evidence
- 36 Security
- 11 Traceability
- 32 Safety standards
- 7 Robots development
- 12 HCI concerns or Human factors or Operator Behavior
- 23 Gray literature
- 26 Risk Assessment or Management
- 80 Dependability or Reliability
- 76 Requirements (RE) activities
- 9 Software Product Lines (SPL)
- 50 Design/Architecture
- 5 Agile Development

111 excluded*:
- 1 Short-paper
- 4 Hazard or Safety analysis
- 1 Safety Assurance or Evidence
- 7 Security
- 15 Traceability
- 1 Safety standards
- 2 Robots development
- 6 Not available
- 14 HCI concerns or Human factors or Operator Behavior
- 3 Redundant paper of same authorship
- 24 Risk Assessment or Management
- 32 Dependability or Reliability
- 2 Requirements (RE) activities
- 20 Software Product Lines (SPL)
- 8 Design/Architecture
- 1 Agile Development

Fig. 2. Paper selection flowchart.

Extraction form

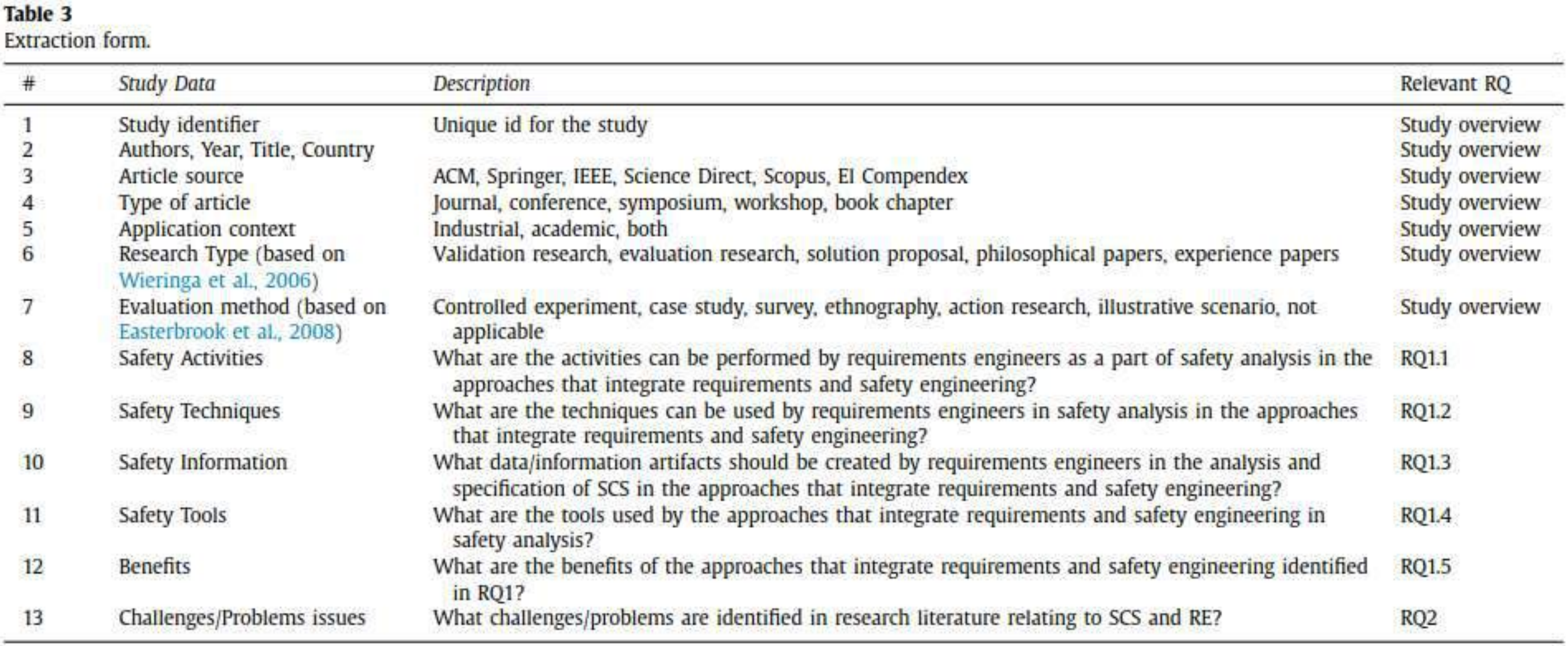


Table 3
Extraction form.

#	*Study Data*	*Description*	Relevant RQ
1	Study identifier	Unique id for the study	Study overview
2	Authors, Year, Title, Country		Study overview
3	Article source	ACM, Springer, IEEE, Science Direct, Scopus, EI Compendex	Study overview
4	Type of article	Journal, conference, symposium, workshop, book chapter	Study overview
5	Application context	Industrial, academic, both	Study overview
6	Research Type (based on Wieringa et al., 2006)	Validation research, evaluation research, solution proposal, philosophical papers, experience papers	Study overview
7	Evaluation method (based on Easterbrook et al., 2008)	Controlled experiment, case study, survey, ethnography, action research, illustrative scenario, not applicable	Study overview
8	Safety Activities	What are the activities can be performed by requirements engineers as a part of safety analysis in the approaches that integrate requirements and safety engineering?	RQ1.1
9	Safety Techniques	What are the techniques can be used by requirements engineers in safety analysis in the approaches that integrate requirements and safety engineering?	RQ1.2
10	Safety Information	What data/information artifacts should be created by requirements engineers in the analysis and specification of SCS in the approaches that integrate requirements and safety engineering?	RQ1.3
11	Safety Tools	What are the tools used by the approaches that integrate requirements and safety engineering in safety analysis?	RQ1.4
12	Benefits	What are the benefits of the approaches that integrate requirements and safety engineering identified in RQ1?	RQ1.5
13	Challenges/Problems issues	What challenges/problems are identified in research literature relating to SCS and RE?	RQ2

Study quality assessment criteria

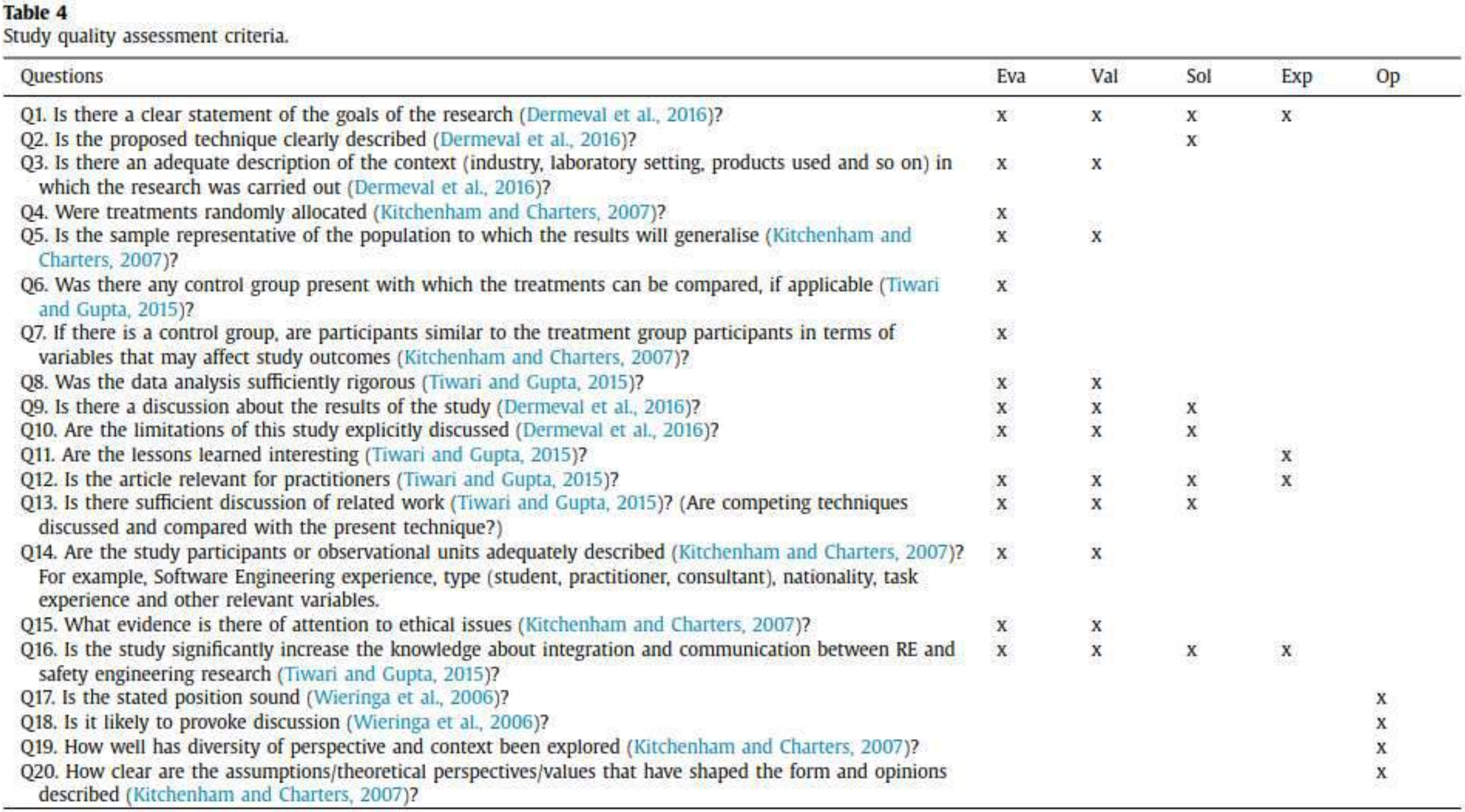


Table 4
Study quality assessment criteria.

Questions	Eva	Val	Sol	Exp	Op
Q1. Is there a clear statement of the goals of the research (Dermeval et al., 2016)?	x	x	x	x	
Q2. Is the proposed technique clearly described (Dermeval et al., 2016)?			x		
Q3. Is there an adequate description of the context (industry, laboratory setting, products used and so on) in which the research was carried out (Dermeval et al., 2016)?	x	x			
Q4. Were treatments randomly allocated (Kitchenham and Charters, 2007)?	x				
Q5. Is the sample representative of the population to which the results will generalise (Kitchenham and Charters, 2007)?	x	x			
Q6. Was there any control group present with which the treatments can be compared, if applicable (Tiwari and Gupta, 2015)?	x				
Q7. If there is a control group, are participants similar to the treatment group participants in terms of variables that may affect study outcomes (Kitchenham and Charters, 2007)?	x				
Q8. Was the data analysis sufficiently rigorous (Tiwari and Gupta, 2015)?	x	x			
Q9. Is there a discussion about the results of the study (Dermeval et al., 2016)?	x	x	x		
Q10. Are the limitations of this study explicitly discussed (Dermeval et al., 2016)?	x	x	x		
Q11. Are the lessons learned interesting (Tiwari and Gupta, 2015)?				x	
Q12. Is the article relevant for practitioners (Tiwari and Gupta, 2015)?	x	x	x	x	
Q13. Is there sufficient discussion of related work (Tiwari and Gupta, 2015)? (Are competing techniques discussed and compared with the present technique?)	x	x	x		
Q14. Are the study participants or observational units adequately described (Kitchenham and Charters, 2007)? For example, Software Engineering experience, type (student, practitioner, consultant), nationality, task experience and other relevant variables.	x	x			
Q15. What evidence is there of attention to ethical issues (Kitchenham and Charters, 2007)?	x	x			
Q16. Is the study significantly increase the knowledge about integration and communication between RE and safety engineering research (Tiwari and Gupta, 2015)?	x	x	x	x	
Q17. Is the stated position sound (Wieringa et al., 2006)?					x
Q18. Is it likely to provoke discussion (Wieringa et al., 2006)?					x
Q19. How well has diversity of perspective and context been explored (Kitchenham and Charters, 2007)?					x
Q20. How clear are the assumptions/theoretical perspectives/values that have shaped the form and opinions described (Kitchenham and Charters, 2007)?					x

Quality assessment results (1)

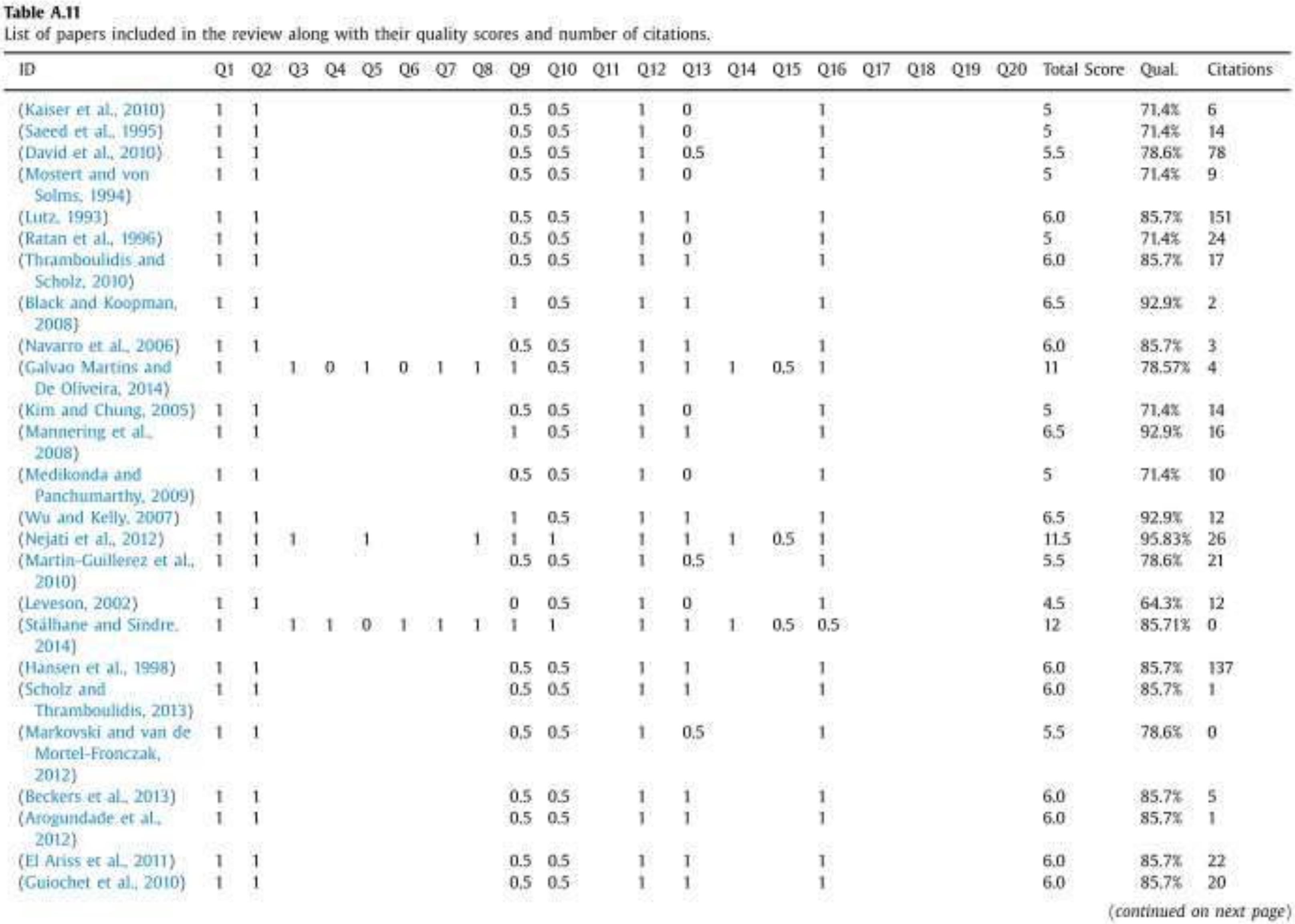


Table A.11
List of papers included in the review along with their quality scores and number of citations.

ID	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Total Score	Qual.	Citations
(Kaiser et al., 2010)	1	1							0.5	0.5		1	0			1					5	71.4%	6
(Saeed et al., 1995)	1	1							0.5	0.5		1	0			1					5	71.4%	14
(David et al., 2010)	1	1							0.5	0.5		1	0.5			1					5.5	78.6%	78
(Mostert and von Solms, 1994)	1	1							0.5	0.5		1	0			1					5	71.4%	9
(Lutz, 1993)	1	1							0.5	0.5		1	1			1					6.0	85.7%	151
(Ratan et al., 1996)	1	1							0.5	0.5		1	0			1					5	71.4%	24
(Thramboulidis and Scholz, 2010)	1	1							0.5	0.5		1	1			1					6.0	85.7%	17
(Black and Koopman, 2008)	1	1							1	0.5		1	1			1					6.5	92.9%	2
(Navarro et al., 2006)	1	1							0.5	0.5		1	1			1					6.0	85.7%	3
(Galvao Martins and De Oliveira, 2014)	1		1	0	1	0	1	1	1	0.5		1	1	1	0.5	1					11	78.57%	4
(Kim and Chung, 2005)	1	1							0.5	0.5		1	0			1					5	71.4%	14
(Mannering et al., 2008)	1	1							1	0.5		1	1			1					6.5	92.9%	16
(Medikonda and Panchumarthy, 2009)	1	1							0.5	0.5		1	0			1					5	71.4%	10
(Wu and Kelly, 2007)	1	1							1	0.5		1	1			1					6.5	92.9%	12
(Nejati et al., 2012)	1	1	1		1			1	1	1		1	1	1	0.5	1					11.5	95.83%	26
(Martin-Guillerez et al., 2010)	1	1							0.5	0.5		1	0.5			1					5.5	78.6%	21
(Leveson, 2002)	1	1							0	0.5		1	0			1					4.5	64.3%	12
(Stålhane and Sindre, 2014)	1		1	1	0	1	1	1	1	1		1	1	1	0.5	0.5					12	85.71%	0
(Hansen et al., 1998)	1	1							0.5	0.5		1	1			1					6.0	85.7%	137
(Scholz and Thramboulidis, 2013)	1	1							0.5	0.5		1	1			1					6.0	85.7%	1
(Markovski and van de Mortel-Fronczak, 2012)	1	1							0.5	0.5		1	0.5			1					5.5	78.6%	0
(Beckers et al., 2013)	1	1							0.5	0.5		1	1			1					6.0	85.7%	5
(Arogundade et al., 2012)	1	1							0.5	0.5		1	1			1					6.0	85.7%	1
(El Ariss et al., 2011)	1	1							0.5	0.5		1	1			1					6.0	85.7%	22
(Guiochet et al., 2010)	1	1							0.5	0.5		1	1			1					6.0	85.7%	20

(*continued on next page*)

Quality assessment results (2)

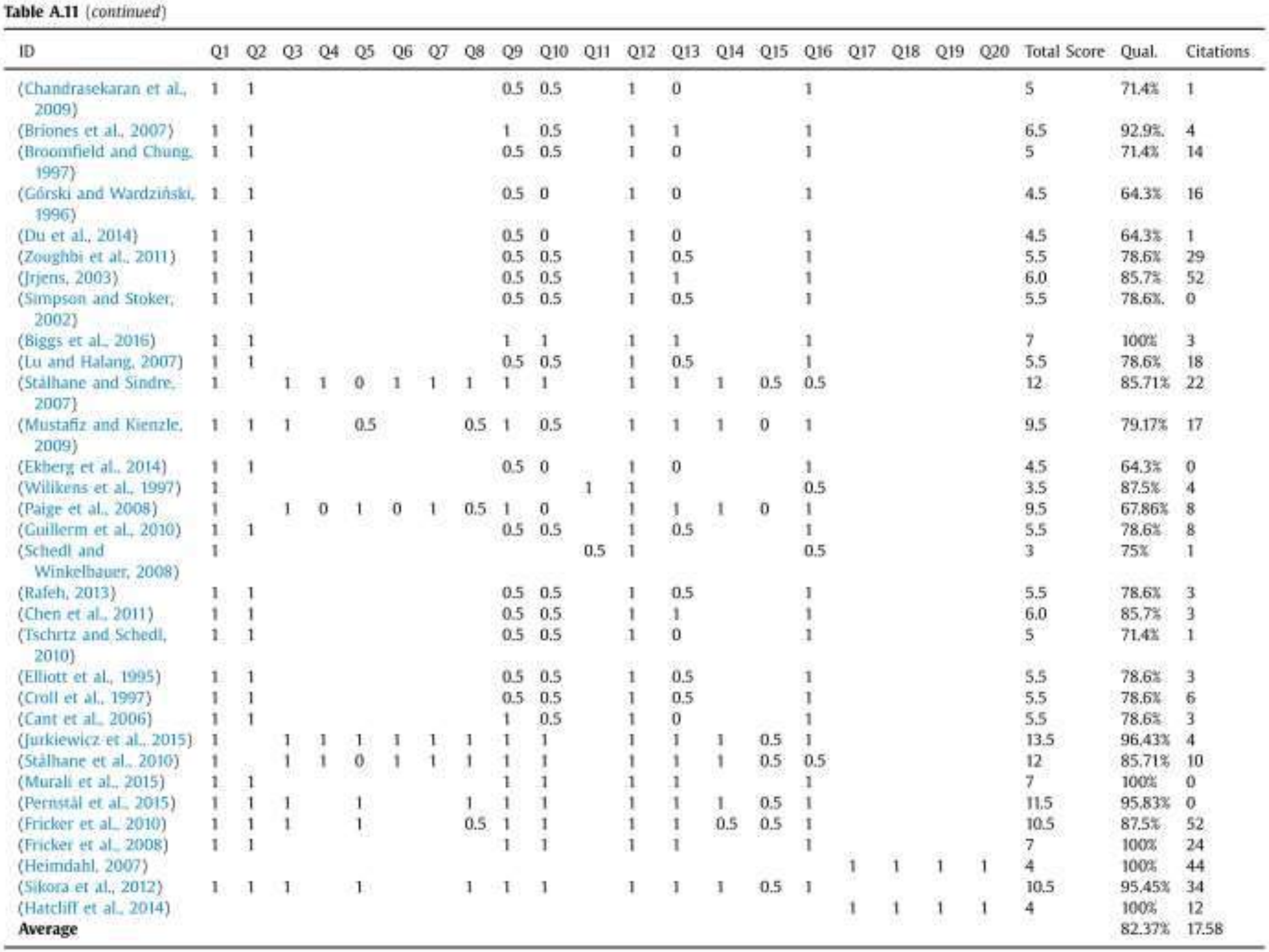


Table A.11 (*continued*)

ID	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Total Score	Qual.	Citations
(Chandrasekaran et al., 2009)	1	1							0.5	0.5		1	0			1					5	71.4%	1
(Briones et al., 2007)	1	1							1	0.5		1	1			1					6.5	92.9%.	4
(Broomfield and Chung, 1997)	1	1							0.5	0.5		1	0			1					5	71.4%	14
(Górski and Wardziński, 1996)	1	1							0.5	0		1	0			1					4.5	64.3%	16
(Du et al., 2014)	1	1							0.5	0		1	0			1					4.5	64.3%	1
(Zoughbi et al., 2011)	1	1							0.5	0.5		1	0.5			1					5.5	78.6%	29
(Jrjens, 2003)	1	1							0.5	0.5		1	1			1					6.0	85.7%	52
(Simpson and Stoker, 2002)	1	1							0.5	0.5		1	0.5			1					5.5	78.6%.	0
(Biggs et al., 2016)	1	1							1	1		1	1			1					7	100%	3
(Lu and Halang, 2007)	1	1							0.5	0.5		1	0.5			1					5.5	78.6%	18
(Stålhane and Sindre, 2007)	1		1	1	0	1	1	1	1	1		1	1	1	0.5	0.5					12	85.71%	22
(Mustafiz and Kienzle, 2009)	1	1	1		0.5			0.5	1	0.5		1	1	1	0	1					9.5	79.17%	17
(Ekberg et al., 2014)	1	1							0.5	0		1	0			1					4.5	64.3%	0
(Wilikens et al., 1997)	1										1	1				0.5					3.5	87.5%	4
(Paige et al., 2008)	1		1	0	1	0	1	0.5	1	0		1	1	1	0	1					9.5	67.86%	8
(Guillerm et al., 2010)	1	1							0.5	0.5		1	0.5			1					5.5	78.6%	8
(Schedl and Winkelbauer, 2008)	1										0.5	1				0.5					3	75%	1
(Rafeh, 2013)	1	1							0.5	0.5		1	0.5			1					5.5	78.6%	3
(Chen et al., 2011)	1	1							0.5	0.5		1	1			1					6.0	85.7%	3
(Tschrtz and Schedl, 2010)	1	1							0.5	0.5		1	0			1					5	71.4%	1
(Elliott et al., 1995)	1	1							0.5	0.5		1	0.5			1					5.5	78.6%	3
(Croll et al., 1997)	1	1							0.5	0.5		1	0.5			1					5.5	78.6%	6
(Cant et al., 2006)	1	1							1	0.5		1	0			1					5.5	78.6%	3
(Jurkiewicz et al., 2015)	1		1	1	1	1	1	1	1	1		1	1	1	0.5	1					13.5	96.43%	4
(Stålhane et al., 2010)	1		1	1	0	1	1	1	1	1		1	1	1	0.5	0.5					12	85.71%	10
(Murali et al., 2015)	1	1							1	1		1	1			1					7	100%	0
(Pernstål et al., 2015)	1	1	1		1			1	1	1		1	1	1	0.5	1					11.5	95.83%	0
(Fricker et al., 2010)	1	1	1		1			0.5	1	1		1	1	0.5	0.5	1					10.5	87.5%	52
(Fricker et al., 2008)	1	1							1	1		1	1			1					7	100%	24
(Heimdahl, 2007)																	1	1	1	1	4	100%	44
(Sikora et al., 2012)	1	1	1		1			1	1	1		1	1	1	0.5	1					10.5	95.45%	34
(Hatcliff et al., 2014)																	1	1	1	1	4	100%	12
Average																						82.37%	17.58

Overview of the studies

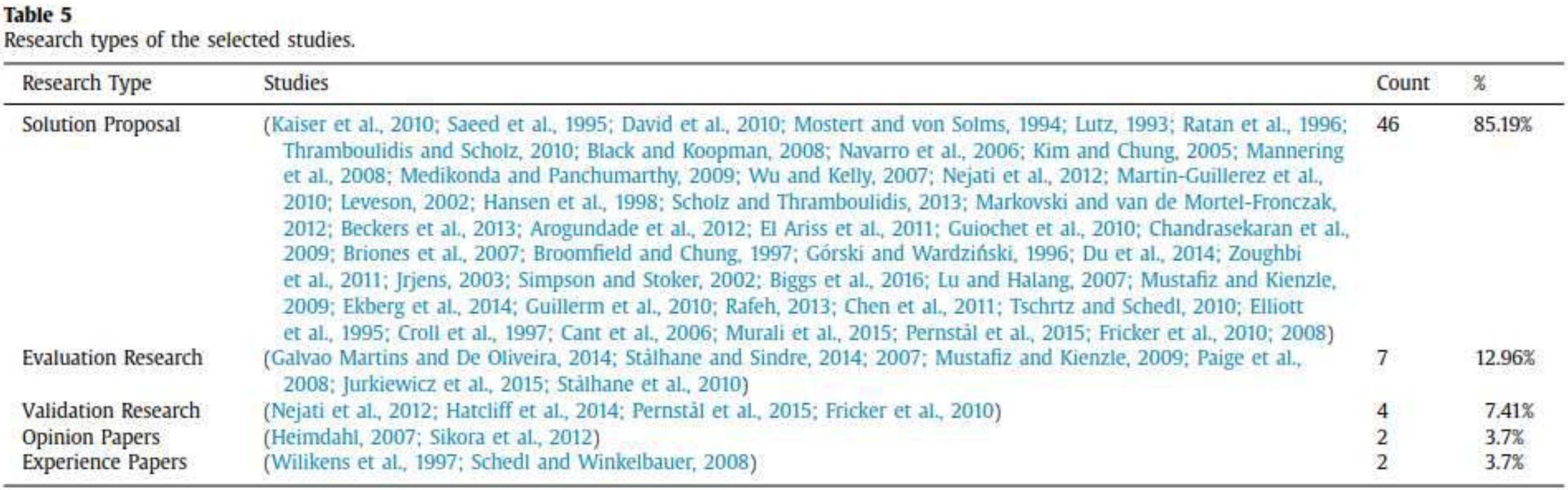


Table 5
Research types of the selected studies.

Research Type	Studies	Count	%
Solution Proposal	(Kaiser et al., 2010; Saeed et al., 1995; David et al., 2010; Mostert and von Solms, 1994; Lutz, 1993; Ratan et al., 1996; Thramboulidis and Scholz, 2010; Black and Koopman, 2008; Navarro et al., 2006; Kim and Chung, 2005; Mannering et al., 2008; Medikonda and Panchumarthy, 2009; Wu and Kelly, 2007; Nejati et al., 2012; Martin-Guillerez et al., 2010; Leveson, 2002; Hansen et al., 1998; Scholz and Thramboulidis, 2013; Markovski and van de Mortel-Fronczak, 2012; Beckers et al., 2013; Arogundade et al., 2012; El Ariss et al., 2011; Guiochet et al., 2010; Chandrasekaran et al., 2009; Briones et al., 2007; Broomfield and Chung, 1997; Górski and Wardziński, 1996; Du et al., 2014; Zoughbi et al., 2011; Jrjens, 2003; Simpson and Stoker, 2002; Biggs et al., 2016; Lu and Halang, 2007; Mustafiz and Kienzle, 2009; Ekberg et al., 2014; Guillerm et al., 2010; Rafeh, 2013; Chen et al., 2011; Tschrtz and Schedl, 2010; Elliott et al., 1995; Croll et al., 1997; Cant et al., 2006; Murali et al., 2015; Pernstål et al., 2015; Fricker et al., 2010; 2008)	46	85.19%
Evaluation Research	(Galvao Martins and De Oliveira, 2014; Stålhane and Sindre, 2014; 2007; Mustafiz and Kienzle, 2009; Paige et al., 2008; Jurkiewicz et al., 2015; Stålhane et al., 2010)	7	12.96%
Validation Research	(Nejati et al., 2012; Hatcliff et al., 2014; Pernstål et al., 2015; Fricker et al., 2010)	4	7.41%
Opinion Papers	(Heimdahl, 2007; Sikora et al., 2012)	2	3.7%
Experience Papers	(Wilikens et al., 1997; Schedl and Winkelbauer, 2008)	2	3.7%

Overview of the studies

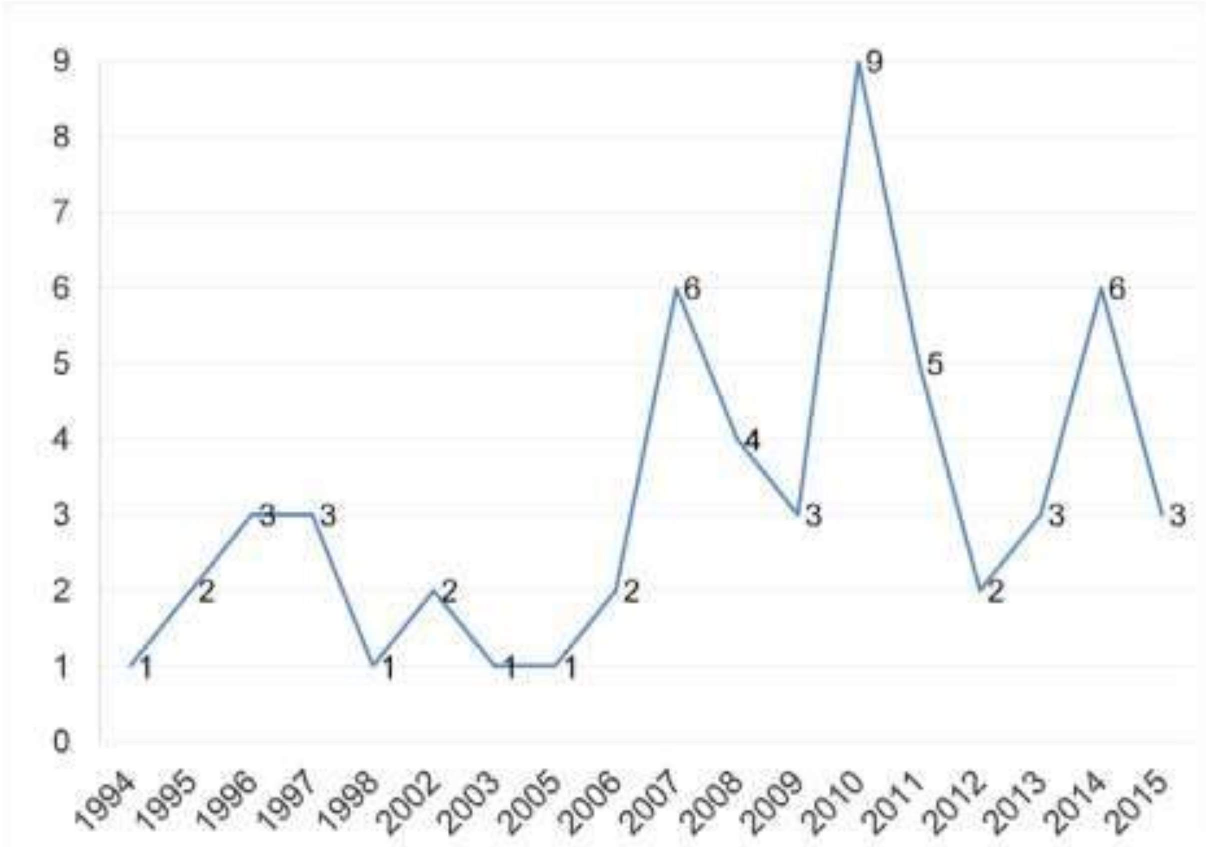


Fig. 3. Temporal view of the studies.

Overview of the studies

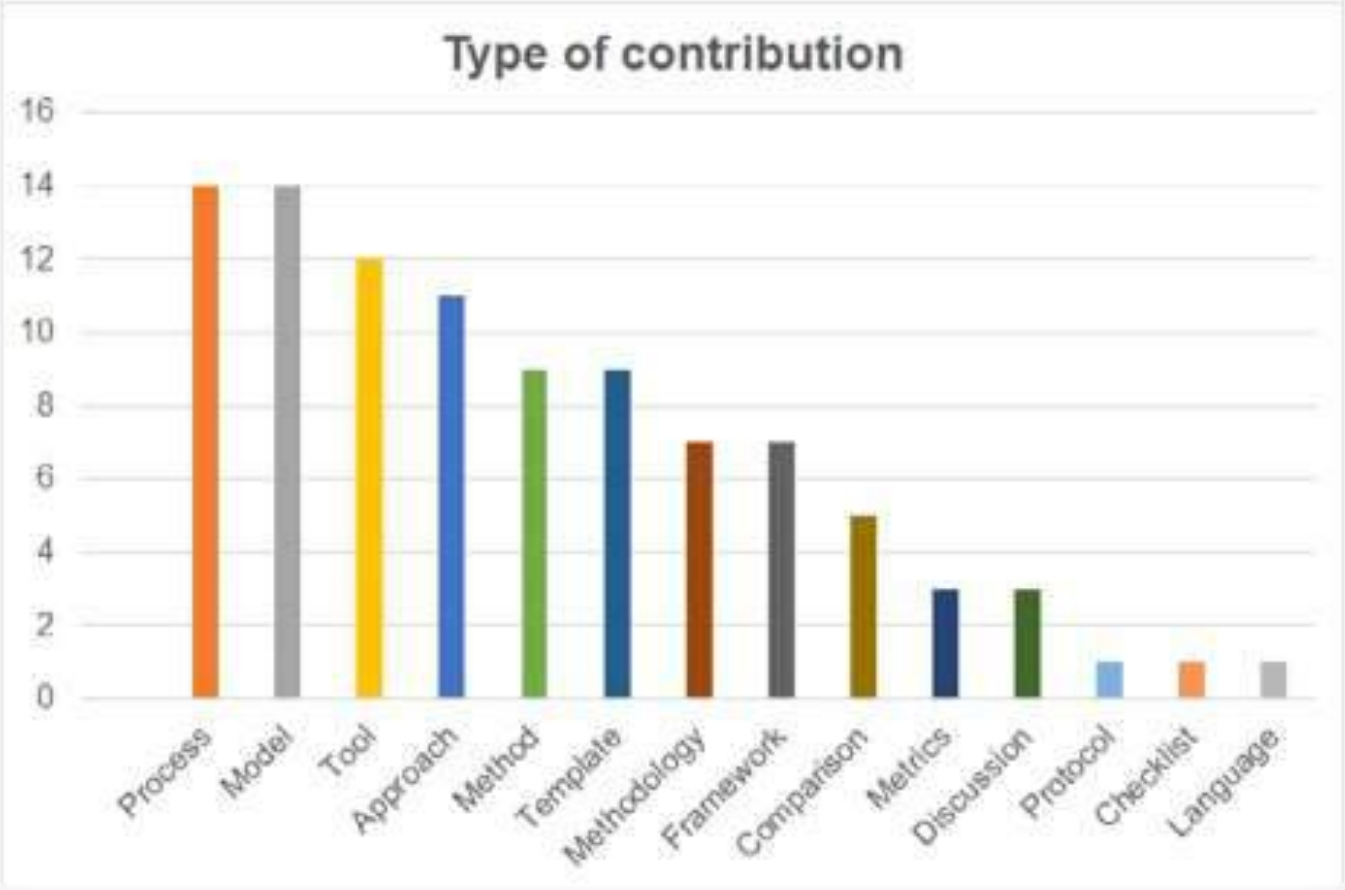


Fig. 4. Types of contributions on integration and communication between RE and safety engineering.

Rigor and relevance analysis [9]

- Rigor:
  - is not the actual rigor of studies, e.g. use of a correct analysis method, that is considered in the model.
  - It is the extent to which aspects related to rigor are presented

- According to the model, the rigor is evaluated through three aspects: Context described, Study design described , and Validity discussed.
  - All these aspects are scored with the same three score levels in a three point scale: 0 (weak), 0.5 (medium), and 1 (strong) description.

Rigor and relevance analysis [9]

- Relevance is evaluated by analyzing four aspects:
  - (1) Subjects that participated in the studies; (2) the Context in which the studies were performed; (3) the Research Method adopted in the studies; and (4) the Scale used in the studies evaluation.

- If the aspect contributes to industrial relevance it receives the score 1, otherwise, it receives 0.

- Therefore, the maximum value for rigor an approach can have is three, while relevance has a maximum of four [9].

Rigor and relevance analysis [9]

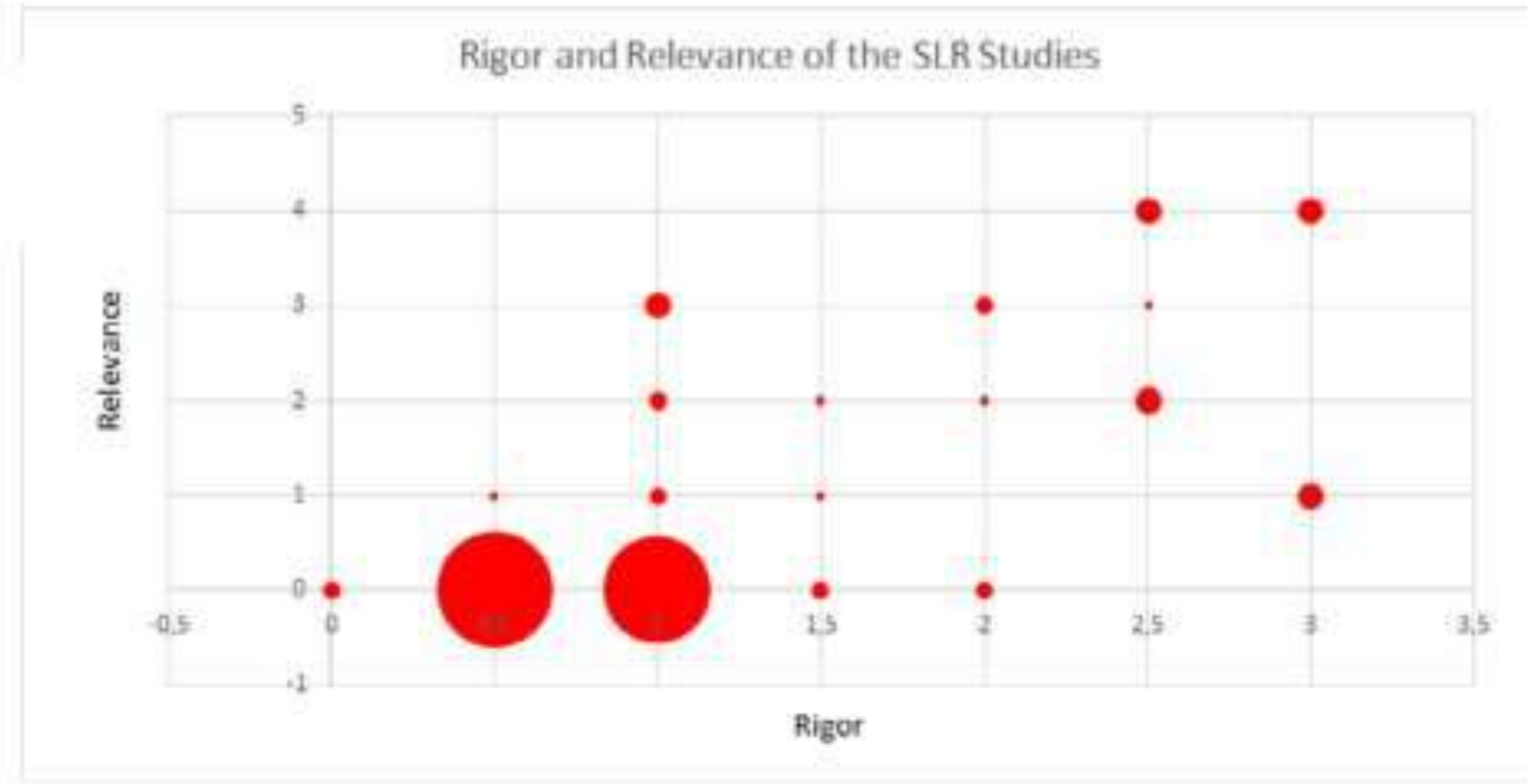


Fig. 5. Rigor and relevance of the approaches.

Rigor and relevance per type of contribution

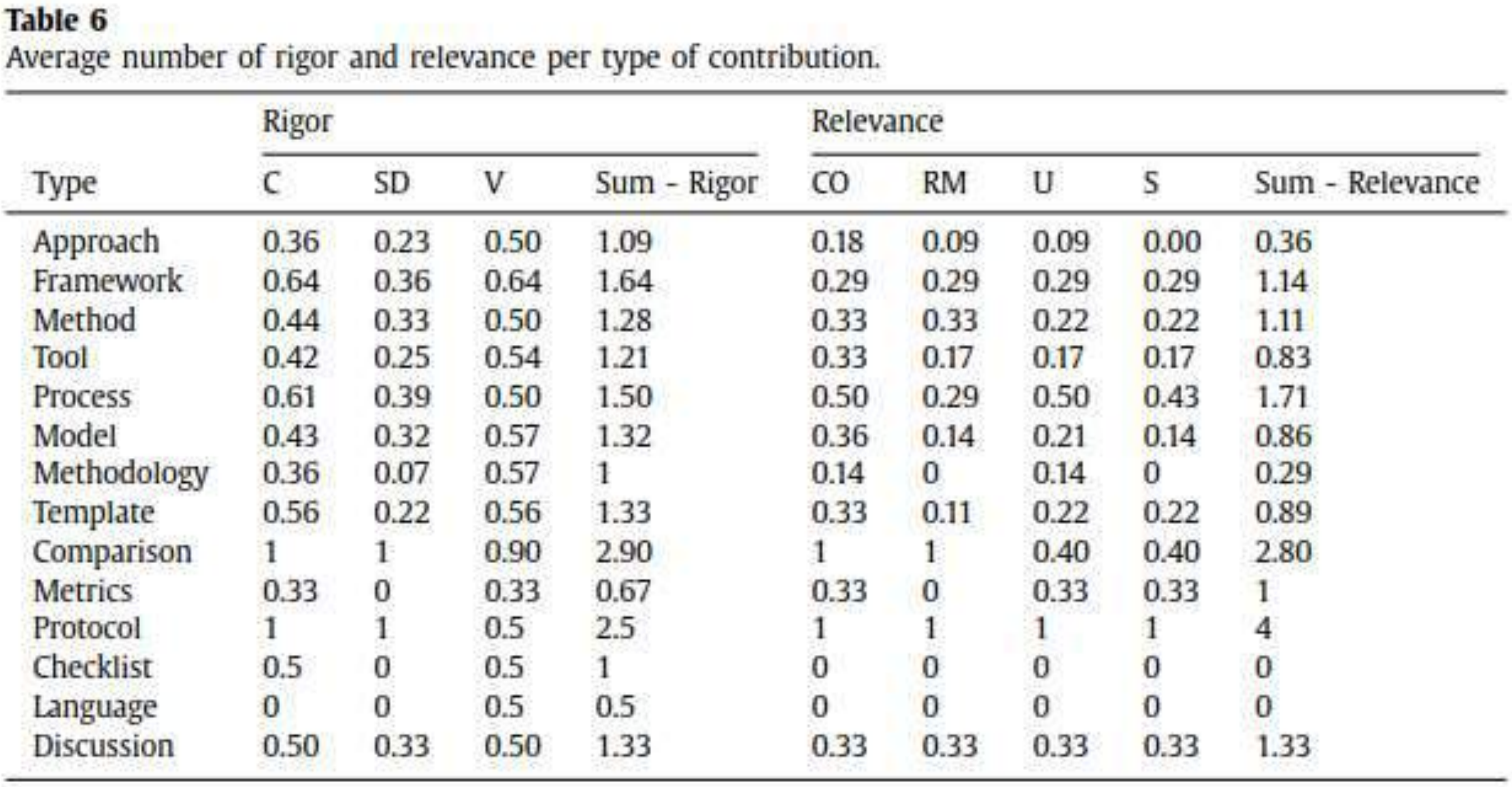


Table 6
Average number of rigor and relevance per type of contribution.

	Rigor				Relevance				
Type	C	SD	V	Sum - Rigor	CO	RM	U	S	Sum - Relevance
Approach	0.36	0.23	0.50	1.09	0.18	0.09	0.09	0.00	0.36
Framework	0.64	0.36	0.64	1.64	0.29	0.29	0.29	0.29	1.14
Method	0.44	0.33	0.50	1.28	0.33	0.33	0.22	0.22	1.11
Tool	0.42	0.25	0.54	1.21	0.33	0.17	0.17	0.17	0.83
Process	0.61	0.39	0.50	1.50	0.50	0.29	0.50	0.43	1.71
Model	0.43	0.32	0.57	1.32	0.36	0.14	0.21	0.14	0.86
Methodology	0.36	0.07	0.57	1	0.14	0	0.14	0	0.29
Template	0.56	0.22	0.56	1.33	0.33	0.11	0.22	0.22	0.89
Comparison	1	1	0.90	2.90	1	1	0.40	0.40	2.80
Metrics	0.33	0	0.33	0.67	0.33	0	0.33	0.33	1
Protocol	1	1	0.5	2.5	1	1	1	1	4
Checklist	0.5	0	0.5	1	0	0	0	0	0
Language	0	0	0.5	0.5	0	0	0	0	0
Discussion	0.50	0.33	0.50	1.33	0.33	0.33	0.33	0.33	1.33

- **Rigor:**
  - □ **Context described (C), Study design described (SD), and Validity discussed (V)**
- **Relevance:**
  - □ **Context (CO), Research method (RM), User/Subject (U), and Scale (S).**

RQ1.1

What are the activities can be performed by requirements engineers as a part of safety analysis in the approaches that integrate requirements and safety engineering?

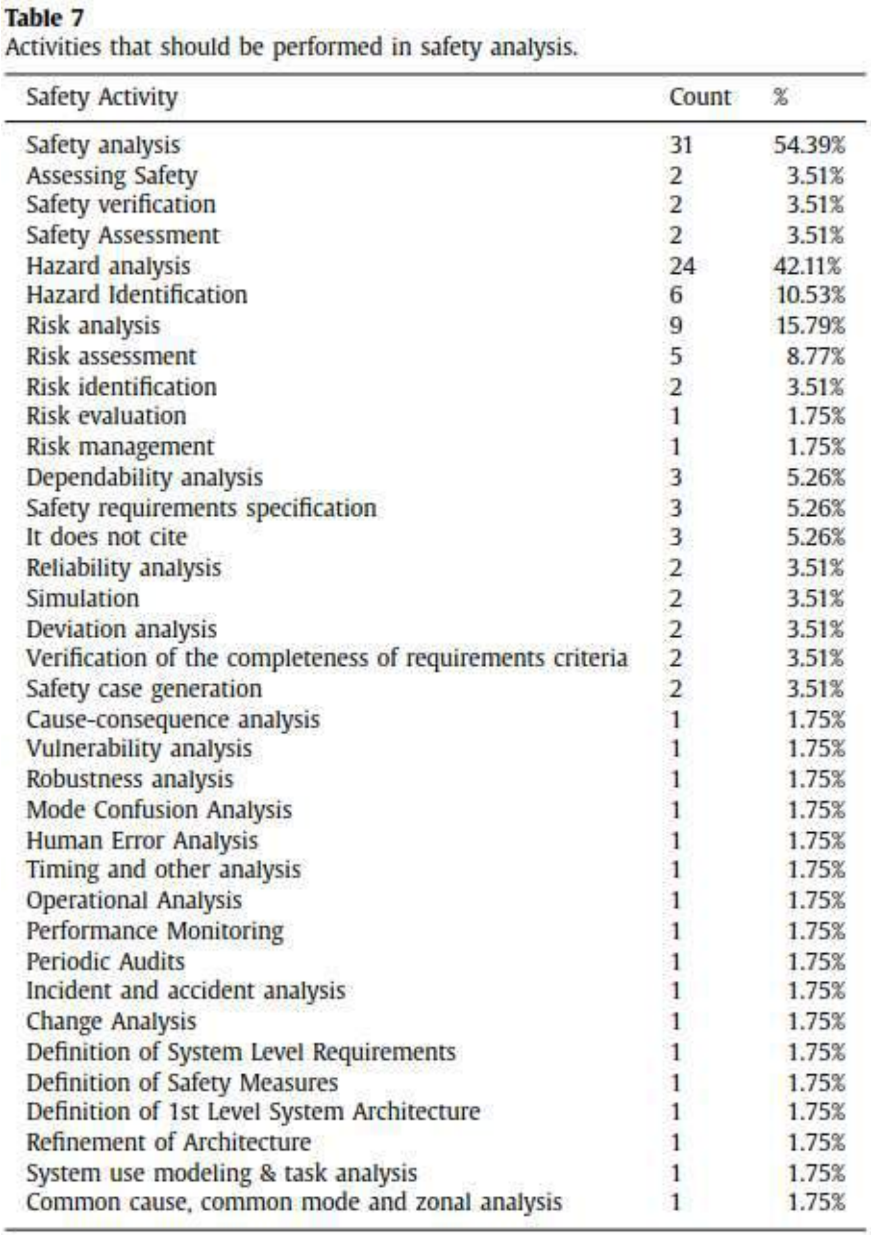


Table 7
Activities that should be performed in safety analysis.

Safety Activity	Count	%
Safety analysis	31	54.39%
Assessing Safety	2	3.51%
Safety verification	2	3.51%
Safety Assessment	2	3.51%
Hazard analysis	24	42.11%
Hazard Identification	6	10.53%
Risk analysis	9	15.79%
Risk assessment	5	8.77%
Risk identification	2	3.51%
Risk evaluation	1	1.75%
Risk management	1	1.75%
Dependability analysis	3	5.26%
Safety requirements specification	3	5.26%
It does not cite	3	5.26%
Reliability analysis	2	3.51%
Simulation	2	3.51%
Deviation analysis	2	3.51%
Verification of the completeness of requirements criteria	2	3.51%
Safety case generation	2	3.51%
Cause-consequence analysis	1	1.75%
Vulnerability analysis	1	1.75%
Robustness analysis	1	1.75%
Mode Confusion Analysis	1	1.75%
Human Error Analysis	1	1.75%
Timing and other analysis	1	1.75%
Operational Analysis	1	1.75%
Performance Monitoring	1	1.75%
Periodic Audits	1	1.75%
Incident and accident analysis	1	1.75%
Change Analysis	1	1.75%
Definition of System Level Requirements	1	1.75%
Definition of Safety Measures	1	1.75%
Definition of 1st Level System Architecture	1	1.75%
Refinement of Architecture	1	1.75%
System use modeling & task analysis	1	1.75%
Common cause, common mode and zonal analysis	1	1.75%

RQ1.2

What are the techniques can be used by requirements engineers during safety analysis in the approaches that integrate requirements and safety engineering?

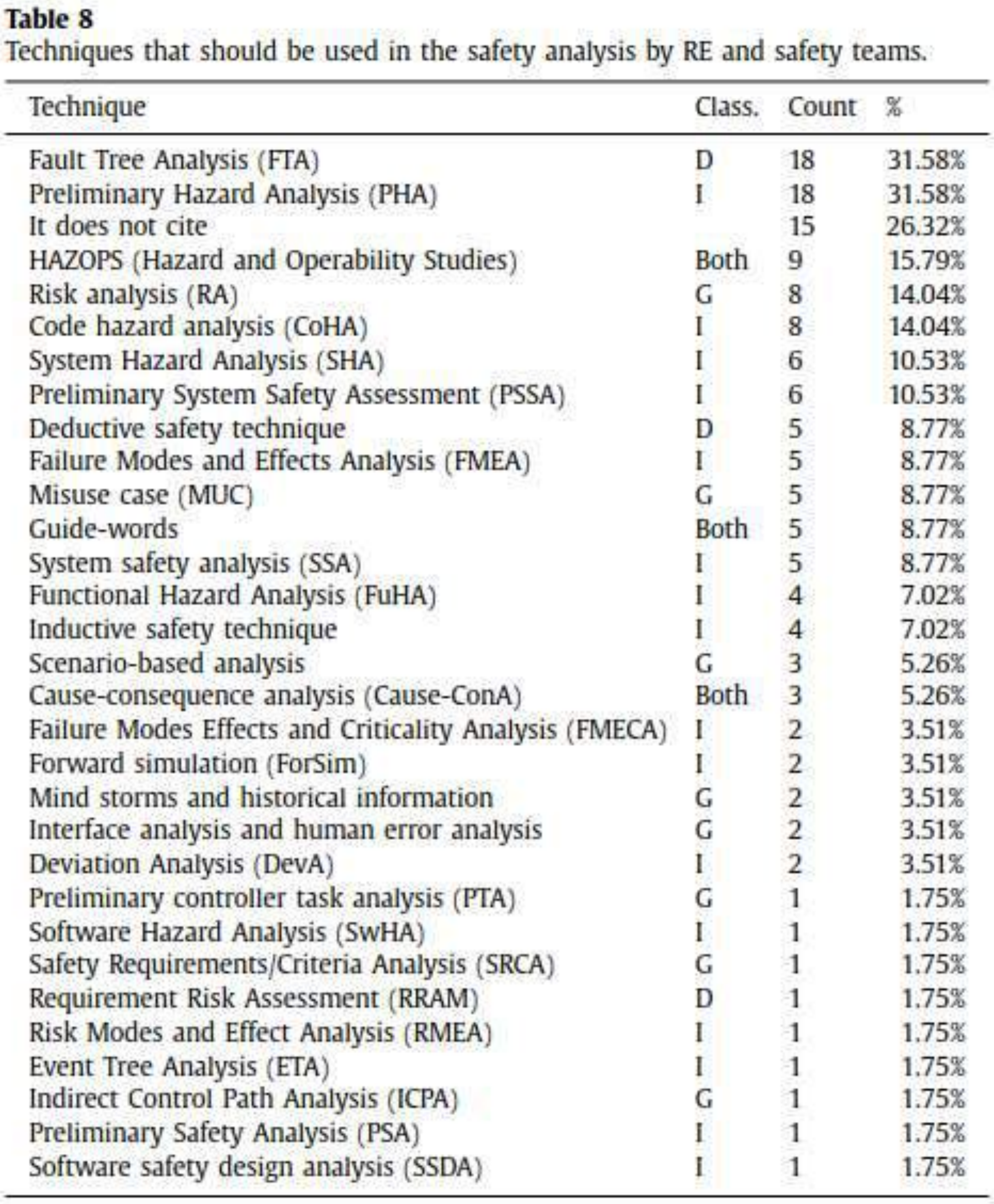
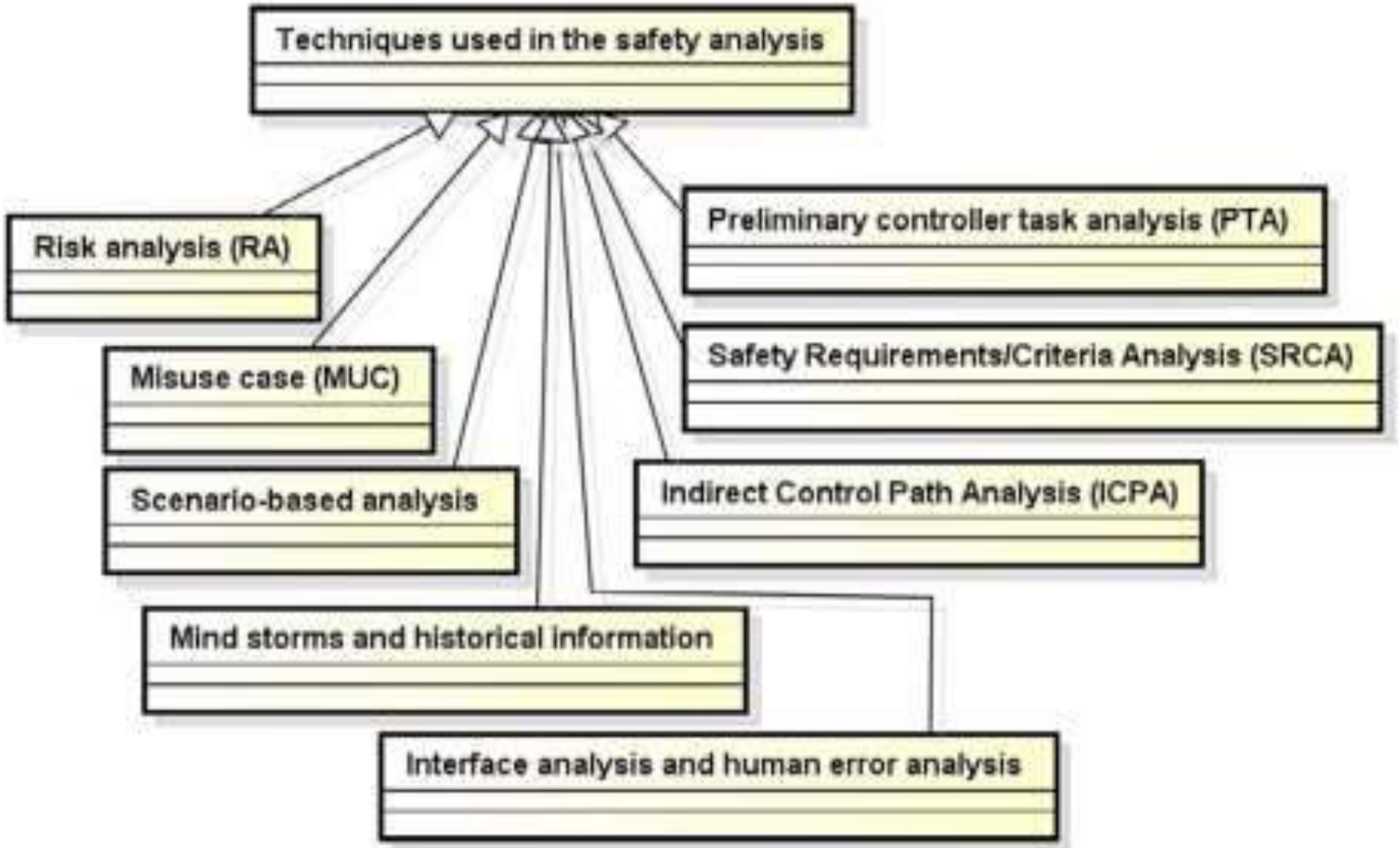


Table 8
Techniques that should be used in the safety analysis by RE and safety teams.

Technique	Class.	Count	%
Fault Tree Analysis (FTA)	D	18	31.58%
Preliminary Hazard Analysis (PHA)	I	18	31.58%
It does not cite		15	26.32%
HAZOPS (Hazard and Operability Studies)	Both	9	15.79%
Risk analysis (RA)	G	8	14.04%
Code hazard analysis (CoHA)	I	8	14.04%
System Hazard Analysis (SHA)	I	6	10.53%
Preliminary System Safety Assessment (PSSA)	I	6	10.53%
Deductive safety technique	D	5	8.77%
Failure Modes and Effects Analysis (FMEA)	I	5	8.77%
Misuse case (MUC)	G	5	8.77%
Guide-words	Both	5	8.77%
System safety analysis (SSA)	I	5	8.77%
Functional Hazard Analysis (FuHA)	I	4	7.02%
Inductive safety technique	I	4	7.02%
Scenario-based analysis	G	3	5.26%
Cause-consequence analysis (Cause-ConA)	Both	3	5.26%
Failure Modes Effects and Criticality Analysis (FMECA)	I	2	3.51%
Forward simulation (ForSim)	I	2	3.51%
Mind storms and historical information	G	2	3.51%
Interface analysis and human error analysis	G	2	3.51%
Deviation Analysis (DevA)	I	2	3.51%
Preliminary controller task analysis (PTA)	G	1	1.75%
Software Hazard Analysis (SwHA)	I	1	1.75%
Safety Requirements/Criteria Analysis (SRCA)	G	1	1.75%
Requirement Risk Assessment (RRAM)	D	1	1.75%
Risk Modes and Effect Analysis (RMEA)	I	1	1.75%
Event Tree Analysis (ETA)	I	1	1.75%
Indirect Control Path Analysis (ICPA)	G	1	1.75%
Preliminary Safety Analysis (PSA)	I	1	1.75%
Software safety design analysis (SSDA)	I	1	1.75%

RQ1.2



Techniques used in the safety analysis
Risk analysis (RA)
Misuse case (MUC)
Scenario-based analysis
Mind storms and historical information
Interface analysis and human error analysis
Preliminary controller task analysis (PTA)
Safety Requirements/Criteria Analysis (SRCA)
Indirect Control Path Analysis (ICPA)

Centro de Informática U·F·P·E

RQ1.2

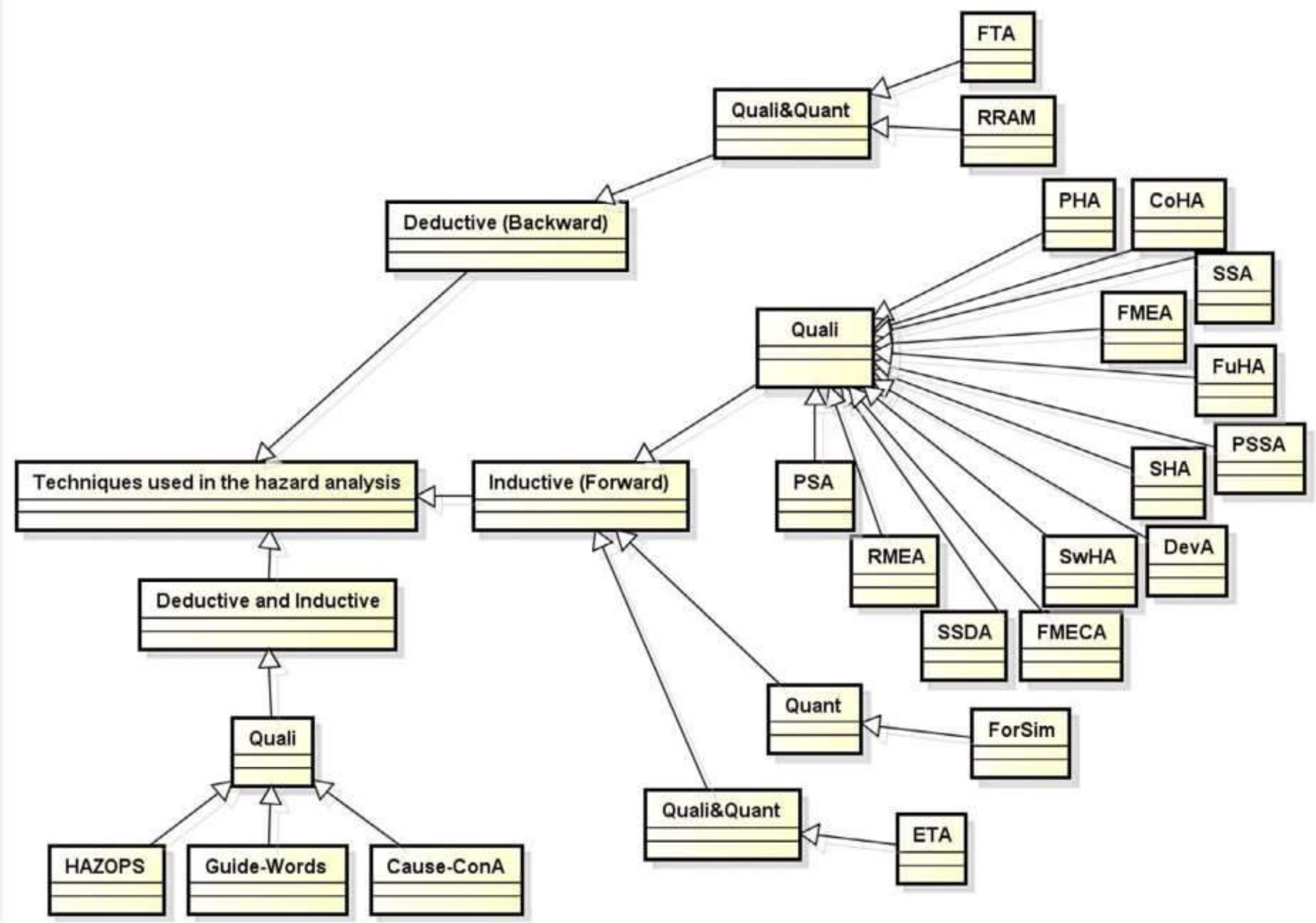


Fig. 7. Taxonomy of techniques used in the hazard analysis according to the selected studies.

RQ1.3

- ***What data/information artifacts can be created by requirements engineers in the analysis and specification of SCS in the approaches that integrate requirements and safety engineering?***

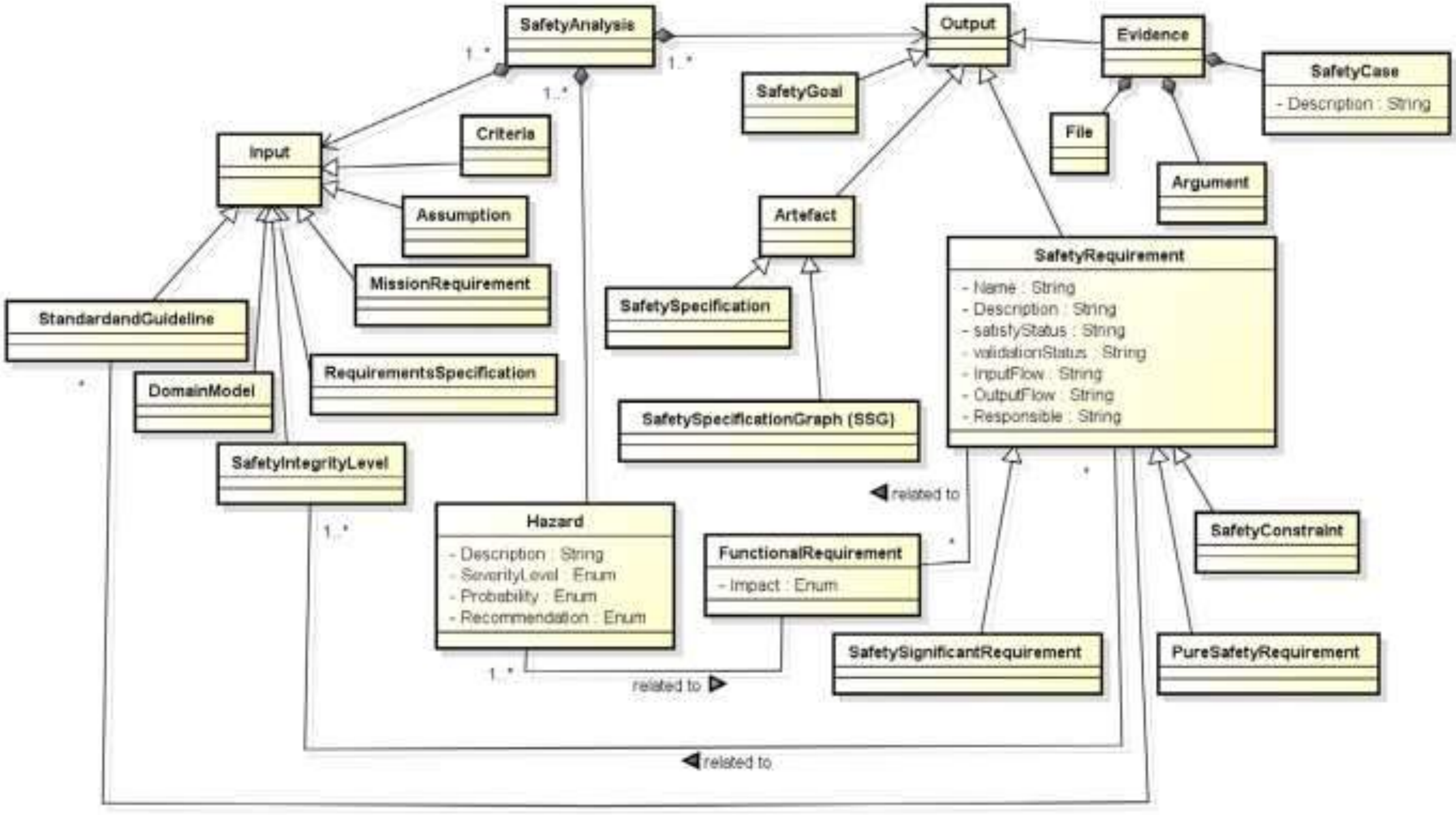
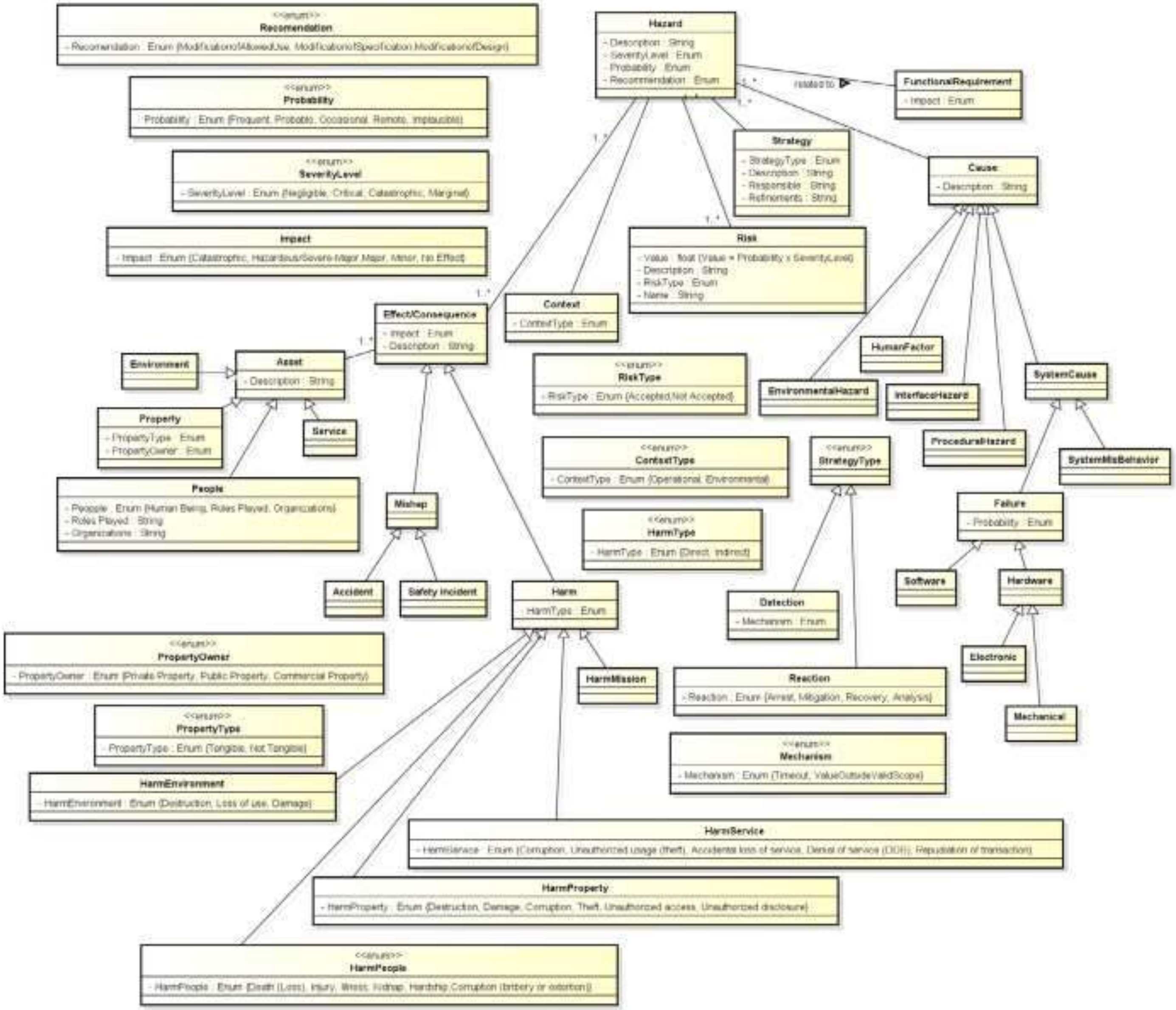


Fig. 8. Safety information taxonomy according to the selected studies.

RQ1.3



<<enum>>
Recomendation
- Recomendation : Enum (ModificationofAllowedUse, ModificationofSpecification,ModificationofDesign)
<<enum>>
Probability
- Probability : Enum (Frequent, Probable, Occasional, Remote, Implausible)
<<enum>>
SeverityLevel
- SeverityLevel : Enum (Negligible, Critical, Catastrophic, Marginal)
Impact
- Impact : Enum (Catastrophic, Hazardous/Severe-Major,Major, Minor, No Effect)
Hazard
- Description : String
- SeverityLevel : Enum
- Probability : Enum
- Recommendation : Enum
related to
FunctionalRequirement
- Impact : Enum
1..*
1..*
1..*
1..*
1..*
1..*
1..*
Strategy
- StrategyType : Enum
- Description : String
- Responsible : String
- Refinements : String
Cause
- Description : String
Risk
- Value : float (Value = Probability x SeverityLevel)
- Description : String
- RiskType : Enum
- Name : String
Context
- ContextType : Enum
Effect/Consequence
- Impact : Enum
- Description : String
Environment
Asset
- Description : String
Property
- PropertyType : Enum
- PropertyOwner : Enum
Service
People
- Peopple : Enum (Human Being, Roles Played, Organizations)
- Roles Played : String
- Organizations : String
Mishap
Accident
Safety Incident
Harm
- HarmType : Enum
HarmMission
<<enum>>
RiskType
- RiskType : Enum (Accepted,Not Accepted)
<<enum>>
ContextType
- ContextType : Enum (Operational, Environmental)
<<enum>>
HarmType
- HarmType : Enum (Direct, Indirect)
<<enum>>
StrategyType
Detection
- Mechanism : Enum
Reaction
- Reaction : Enum (Arrest, Mitigation, Recovery, Analysis)
<<enum>>
Mechanism
- Mechanism : Enum (Timeout, ValueOutsideValidScope)
HumanFactor
EnvironmentalHazard
InterfaceHazard
ProceduralHazard
SystemCause
SystemMisBehavior
Failure
- Probability : Enum
Software
Hardware
Electronic
Mechanical
<<enum>>
PropertyOwner
- PropertyOwner : Enum (Private Property, Public Property, Commercial Property)
<<enum>>
PropertyType
- PropertyType : Enum (Tangible, Not Tangible)
HarmEnvironment
- HarmEnvironment : Enum (Destruction, Loss of use, Damage)
HarmService
- HarmService : Enum (Corruption, Unauthorized usage (theft), Accidental loss of service, Denial of service (DOS), Repudiation of transaction)
HarmProperty
- HarmProperty : Enum (Destruction, Damage, Corruption, Theft, Unauthorized access, Unauthorized disclosure)
<<enum>>
HarmPeople
- HarmPeople : Enum (Death (Loss), Injury, Illness, Kidnap, Hardship,Corruption (bribery or extortion))

Fig. 9. Hazard information taxonomy according to the selected studies.

RQ1.4

What are the tools used by the approaches that integrate requirements and safety engineering in safety analysis?

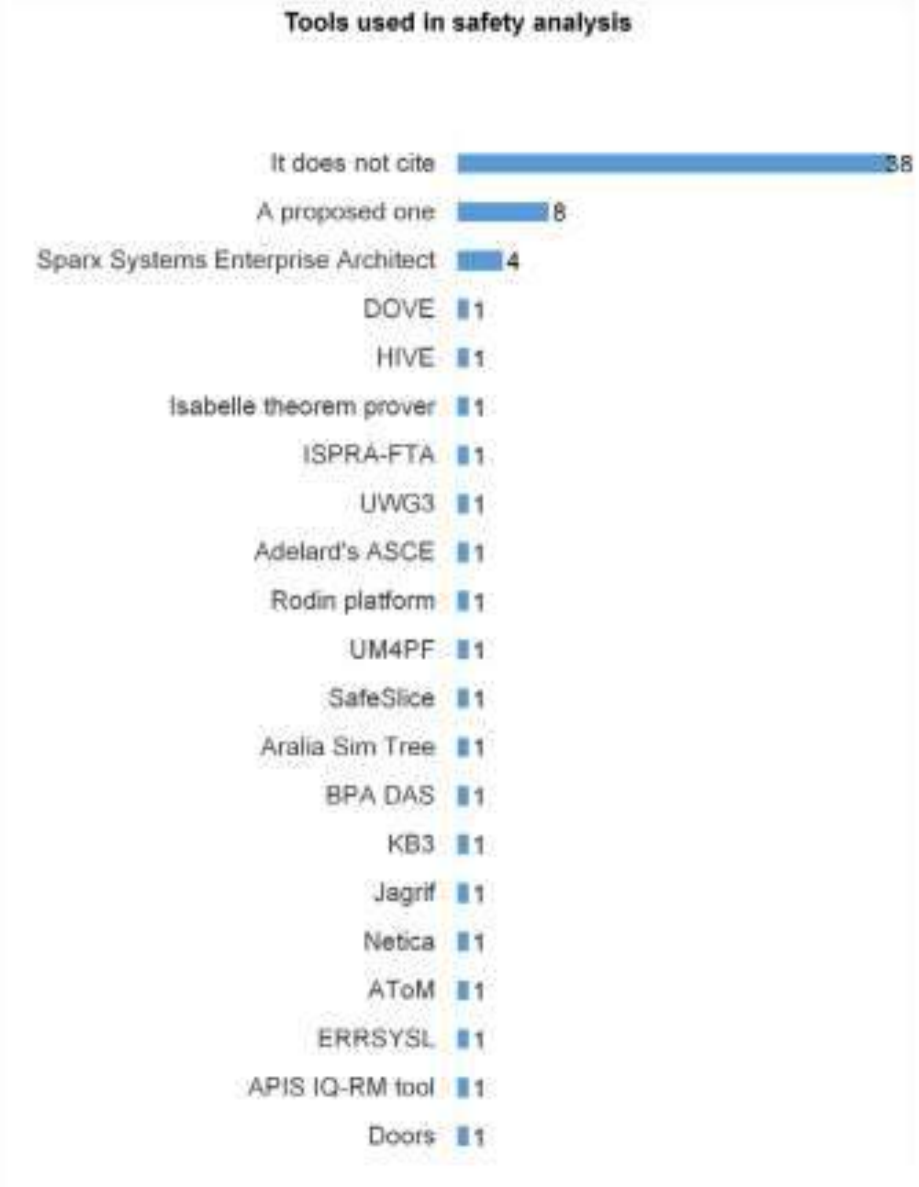


Fig. 10. Tools used in safety analysis.

RQ1.5

What are the benefits of the approaches that integrate requirements and safety engineering identified in RQ1?

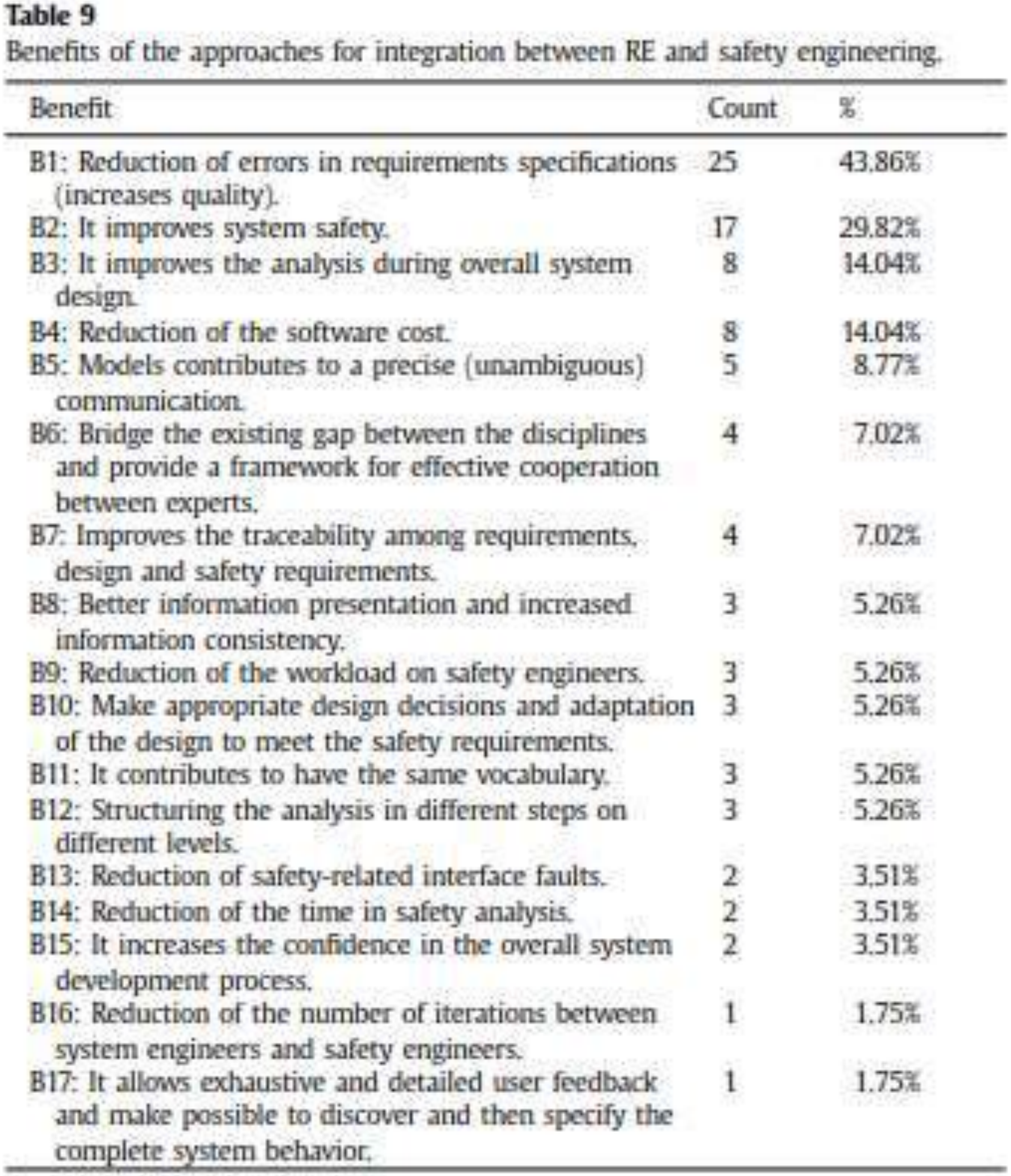


Table 9
Benefits of the approaches for integration between RE and safety engineering.

Benefit	Count	%
B1: Reduction of errors in requirements specifications (increases quality).	25	43.86%
B2: It improves system safety.	17	29.82%
B3: It improves the analysis during overall system design.	8	14.04%
B4: Reduction of the software cost.	8	14.04%
B5: Models contributes to a precise (unambiguous) communication.	5	8.77%
B6: Bridge the existing gap between the disciplines and provide a framework for effective cooperation between experts.	4	7.02%
B7: Improves the traceability among requirements, design and safety requirements.	4	7.02%
B8: Better information presentation and increased information consistency.	3	5.26%
B9: Reduction of the workload on safety engineers.	3	5.26%
B10: Make appropriate design decisions and adaptation of the design to meet the safety requirements.	3	5.26%
B11: It contributes to have the same vocabulary.	3	5.26%
B12: Structuring the analysis in different steps on different levels.	3	5.26%
B13: Reduction of safety-related interface faults.	2	3.51%
B14: Reduction of the time in safety analysis.	2	3.51%
B15: It increases the confidence in the overall system development process.	2	3.51%
B16: Reduction of the number of iterations between system engineers and safety engineers.	1	1.75%
B17: It allows exhaustive and detailed user feedback and make possible to discover and then specify the complete system behavior.	1	1.75%

RQ2

- ***What challenges/problems are identified in research literature relating to SCS and RE?***

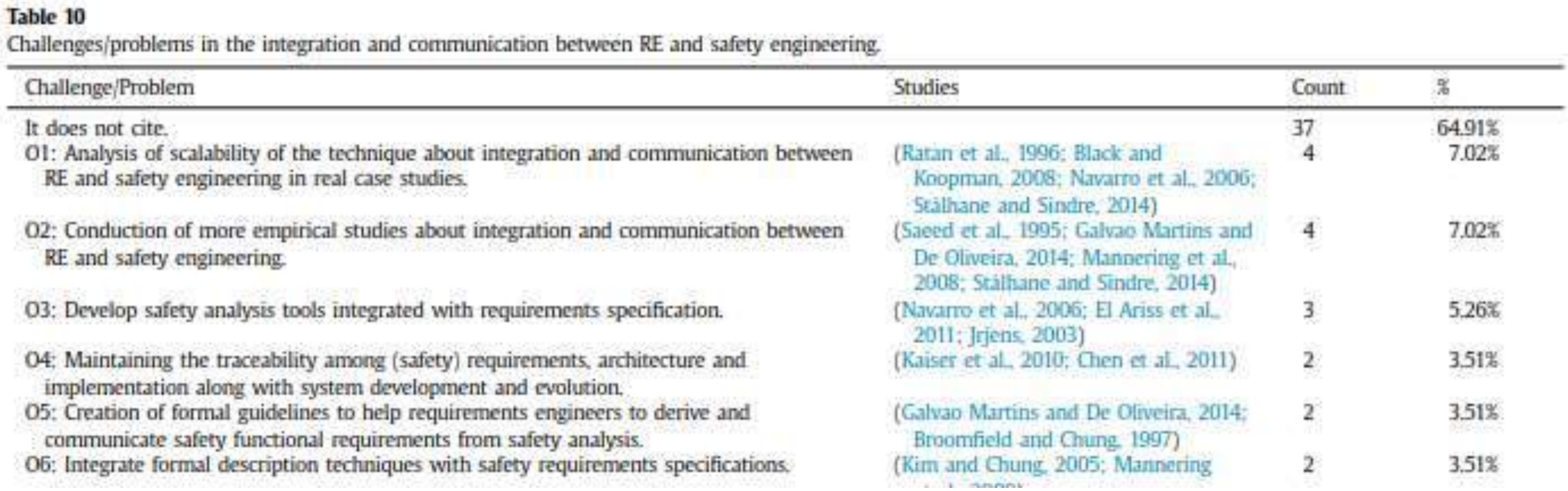
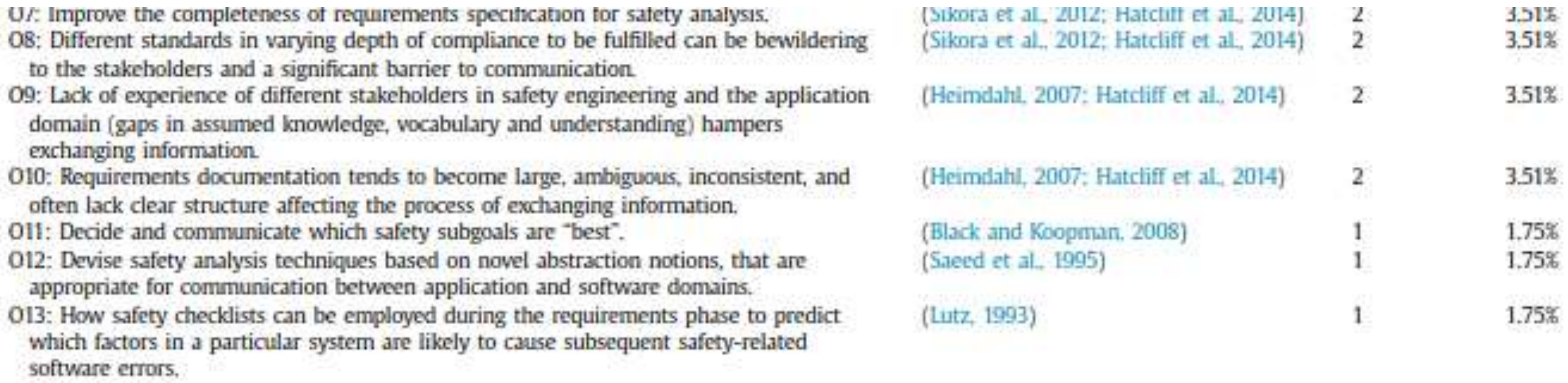


Table 10
Challenges/problems in the integration and communication between RE and safety engineering.

Challenge/Problem	Studies	Count	%
It does not cite.		37	64.91%
O1: Analysis of scalability of the technique about integration and communication between RE and safety engineering in real case studies.	(Ratan et al., 1996; Black and Koopman, 2008; Navarro et al., 2006; Stålhane and Sindre, 2014)	4	7.02%
O2: Conduction of more empirical studies about integration and communication between RE and safety engineering.	(Saeed et al., 1995; Galvao Martins and De Oliveira, 2014; Mannering et al., 2008; Stålhane and Sindre, 2014)	4	7.02%
O3: Develop safety analysis tools integrated with requirements specification.	(Navarro et al., 2006; El Ariss et al., 2011; Jrjens, 2003)	3	5.26%
O4: Maintaining the traceability among (safety) requirements, architecture and implementation along with system development and evolution.	(Kaiser et al., 2010; Chen et al., 2011)	2	3.51%
O5: Creation of formal guidelines to help requirements engineers to derive and communicate safety functional requirements from safety analysis.	(Galvao Martins and De Oliveira, 2014; Broomfield and Chung, 1997)	2	3.51%
O6: Integrate formal description techniques with safety requirements specifications.	(Kim and Chung, 2005; Mannering	2	3.51%

RQ2

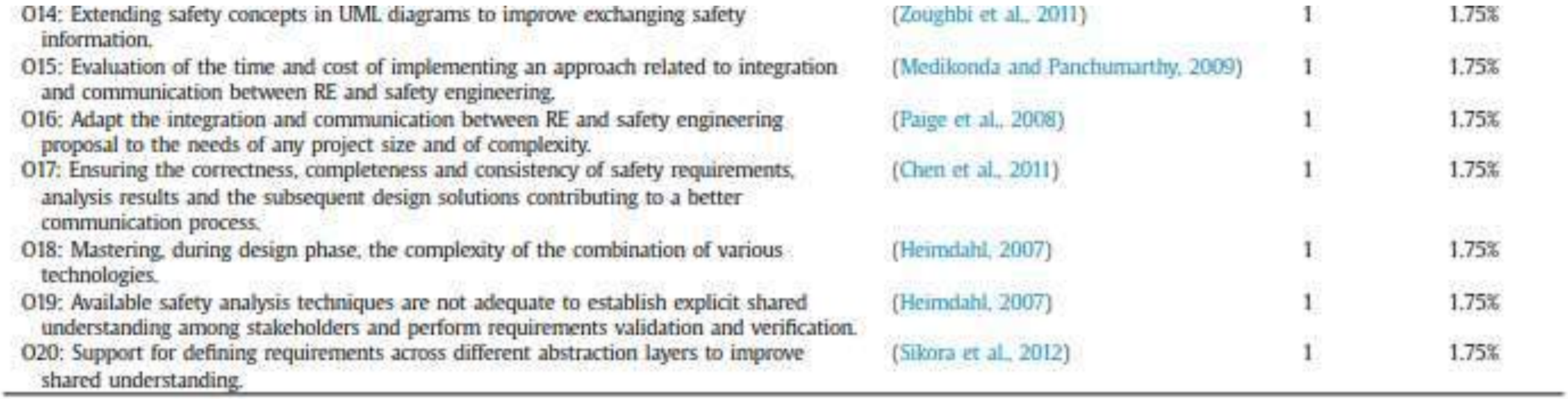
- ***What challenges/problems are identified in research literature relating to SCS and RE?***



O7: Improve the completeness of requirements specification for safety analysis.	(Sikora et al., 2012; Hatcliff et al., 2014)	2	3.51%
O8: Different standards in varying depth of compliance to be fulfilled can be bewildering to the stakeholders and a significant barrier to communication.	(Sikora et al., 2012; Hatcliff et al., 2014)	2	3.51%
O9: Lack of experience of different stakeholders in safety engineering and the application domain (gaps in assumed knowledge, vocabulary and understanding) hampers exchanging information.	(Heimdahl, 2007; Hatcliff et al., 2014)	2	3.51%
O10: Requirements documentation tends to become large, ambiguous, inconsistent, and often lack clear structure affecting the process of exchanging information.	(Heimdahl, 2007; Hatcliff et al., 2014)	2	3.51%
O11: Decide and communicate which safety subgoals are "best".	(Black and Koopman, 2008)	1	1.75%
O12: Devise safety analysis techniques based on novel abstraction notions, that are appropriate for communication between application and software domains.	(Saeed et al., 1995)	1	1.75%
O13: How safety checklists can be employed during the requirements phase to predict which factors in a particular system are likely to cause subsequent safety-related software errors.	(Lutz, 1993)	1	1.75%

RQ2

- ***What challenges/problems are identified in research literature relating to SCS and RE?***



O14: Extending safety concepts in UML diagrams to improve exchanging safety information.	(Zoughbi et al., 2011)	1	1.75%
O15: Evaluation of the time and cost of implementing an approach related to integration and communication between RE and safety engineering.	(Medikonda and Panchumarthy, 2009)	1	1.75%
O16: Adapt the integration and communication between RE and safety engineering proposal to the needs of any project size and of complexity.	(Paige et al., 2008)	1	1.75%
O17: Ensuring the correctness, completeness and consistency of safety requirements, analysis results and the subsequent design solutions contributing to a better communication process.	(Chen et al., 2011)	1	1.75%
O18: Mastering, during design phase, the complexity of the combination of various technologies.	(Heimdahl, 2007)	1	1.75%
O19: Available safety analysis techniques are not adequate to establish explicit shared understanding among stakeholders and perform requirements validation and verification.	(Heimdahl, 2007)	1	1.75%
O20: Support for defining requirements across different abstraction layers to improve shared understanding.	(Sikora et al., 2012)	1	1.75%

Conclusions

- Non-standardization of nomenclature.
- Need of improving the completeness of requirements specification for safety analysis.
- Compliance with safety standards.
- Need of improving safety analysis techniques.
- Need of developing and maintaining traceability mechanisms for safety requirements.
- Need of integration tools.
- Need of more integration between researchers and practitioners.

References

[1] N. G. Leveson. Software safety: Why, what, and how? ACM Computing Surveys, 18(2), June 1986.

[2] N. G. Leveson. Safeware: System Safety and Computers. Addison Wesley, 1995.

[3] Lutz, Robyn R. "Software engineering for safety: a roadmap." In: Proceedings of the Conference on the Future of Software Engineering, 2000, pp. 213-226.

[4] Heimdahl, Mats PE. "Safety and software intensive systems: Challenges old and new." In: Future of Software Engineering, 2007, pp. 137-152.

[5] Sikora, Ernst, Bastian Tenbergen, and Klaus Pohl. "Industry needs and research directions in requirements engineering for embedded systems." Requirements Engineering 17, no. 1 , 2012, pp. 57-78.

References

[6] Hatcliff, John, Alan Wassyng, Tim Kelly, Cyrille Comar, and Paul Jones. "Certifiably safe software-dependent systems: challenges and directions." In Proceedings of the on Future of Software Engineering, 2014, pp. 182-200.

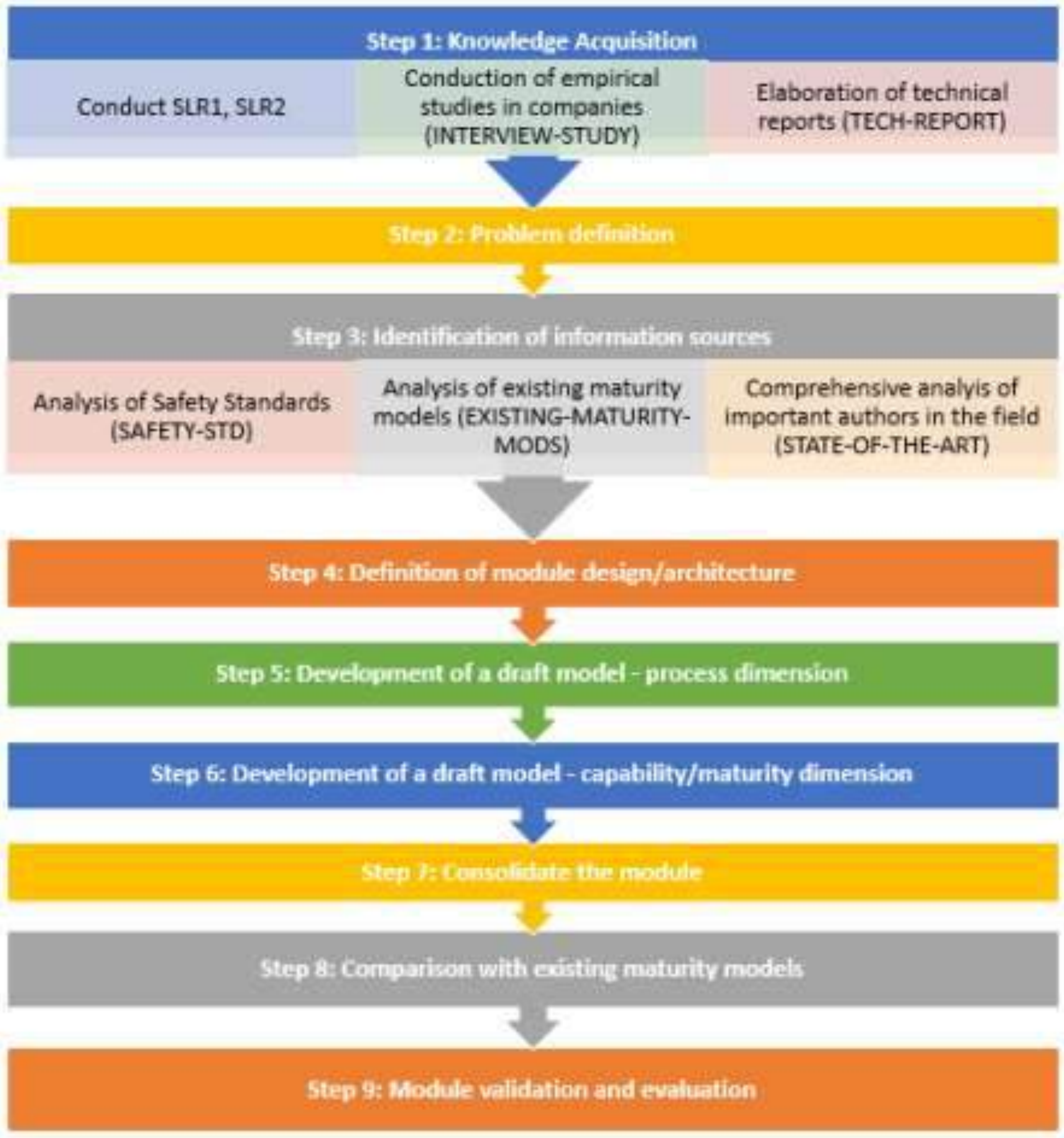
[7] Vilela, Jéssyka, Jaelson Castro, Luiz Eduardo G. Martins, Tony Gorschek, and Carla Silva. "Specifying Safety Requirements with GORE languages." In Proceedings of the 31st Brazilian Symposium on Software Engineering, 2017, pp. 154-163.

[8] VILELA, J., CASTRO, J., MARTINS, L. E. G., GORSCHEK, T. Integration between requirements engineering and safety analysis: A systematic literature review. Journal of Systems and Software, v. 125, 2017, pp. 68-92.

[9] Ivarsson, M. , Gorschek, T. , 2011. A method for evaluating rigor and industrial relevance of technology evaluations. Empirical Softw. Eng. 16 (3), 365–395 .

Research Questions

- RQ1: Which safety practices are suitable to be used in the requirements engineering process of safety-critical systems?
- RQ2: How to design a safety maturity module for the requirements engineering process of safety-critical systems?
- RQ3: How does the proposed safety maturity module compare with related solutions?
- RQ4: What is the effect of applying Uni-REPM Safety module when it is instantiated in different safety-critical domains?
- RQ5: What is the perceived usefulness and ease of use of the Uni-REPM Safety module?
- RQ6: How to evaluate whether the module has a sufficient complete coverage of safety practices?



Step 1: Knowledge Acquisition

Conduct SLR1, SLR2

Conduction of empirical studies in companies (INTERVIEW-STUDY)

Elaboration of technical reports (TECH-REPORT)

Step 2: Problem definition

Step 3: Identification of information sources

Analysis of Safety Standards (SAFETY-STD)

Analysis of existing maturity models (EXISTING-MATURITY-MODS)

Comprehensive analyis of important authors in the field (STATE-OF-THE-ART)

Step 4: Definition of module design/architecture

Step 5: Development of a draft model - process dimension

Step 6: Development of a draft model - capability/maturity dimension

Step 7: Consolidate the module

Step 8: Comparison with existing maturity models

Step 9: Module validation and evaluation

Figure 3.2: Methodology for creating the Uni-REPM Safety module.

The Safety Module and its relationship with Uni-REPM

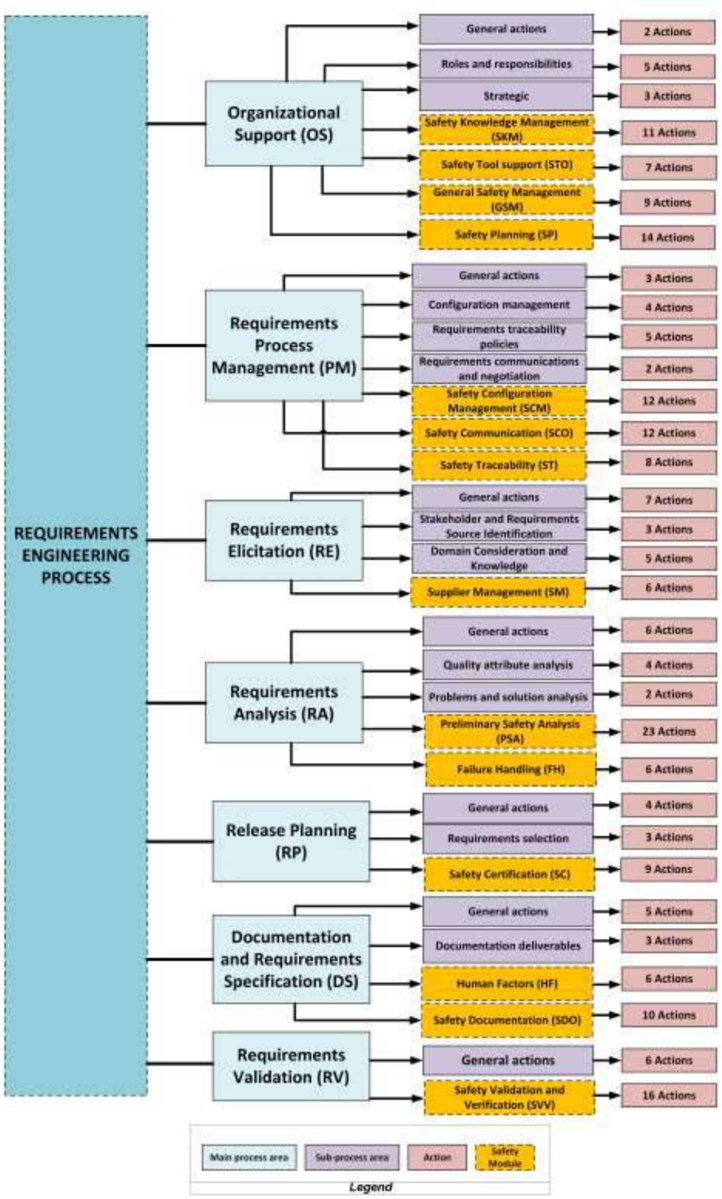

REQUIREMENTS ENGINEERING PROCESS
Organizational Support (OS)
General actions
2 Actions
Roles and responsibilities
5 Actions
Strategic
3 Actions
Safety Knowledge Management (SKM)
11 Actions
Safety Tool support (STO)
7 Actions
General Safety Management (GSM)
9 Actions
Safety Planning (SP)
14 Actions
Requirements Process Management (PM)
General actions
3 Actions
Configuration management
4 Actions
Requirements traceability policies
5 Actions
Requirements communications and negotiation
2 Actions
Safety Configuration Management (SCM)
12 Actions
Safety Communication (SCO)
12 Actions
Safety Traceability (ST)
8 Actions
Requirements Elicitation (RE)
General actions
7 Actions
Stakeholder and Requirements Source Identification
3 Actions
Domain Consideration and Knowledge
5 Actions
Supplier Management (SM)
6 Actions
Requirements Analysis (RA)
General actions
6 Actions
Quality attribute analysis
4 Actions
Problems and solution analysis
2 Actions
Preliminary Safety Analysis (PSA)
23 Actions
Failure Handling (FH)
6 Actions
Release Planning (RP)
General actions
4 Actions
Requirements selection
3 Actions
Safety Certification (SC)
9 Actions
Documentation and Requirements Specification (DS)
General actions
5 Actions
Documentation deliverables
3 Actions
Human Factors (HF)
6 Actions
Safety Documentation (SDO)
10 Actions
Requirements Validation (RV)
General actions
6 Actions
Safety Validation and Verification (SVV)
16 Actions
Main process area
Sub-process area
Action
Safety Module
Legend

Figure 4.2: Safety module and its relationship with Uni-REPM.