On the Use of Safety Certification Practices in Autonomous Field Robot Software Development

Mogensen, Johann Thor Ingibergsson; Schultz, Ulrik Pagh; Kuhrmann, Marco

Published in:
Product-Focused Software Process Improvement

DOI:
10.1007/978-3-319-26844-6_25

Publication date:
2015

Document Version
Early version, also known as pre-print

On the Use of Safety Certification Practices in Autonomous Field Robot Software Development: A Systematic Mapping Study

Johann Thor Mogensen Ingibergsson, Ulrik Pagh Schultz, Marco Kuhrmann

Mærsk Mc-Kinney Møller Institute, University of Southern Denmark
Campusvej 55, 5230 Odense M, Denmark
{jomo|ups|kuhrmann}@mmmi.sdu.dk

Abstract. Robotics has recently seen an increasing development, and the areas addressed within robotics has extended into domains we consider safety-critical, fostering the development of standards that facilitate the development of safe robots. Safety standards describe concepts to maintain desired reactions or performance in malfunctioning systems, and influence industry regarding software development and project management. However, academia seemingly did not reach the same degree of utilisation of standards. This paper presents the findings from a systematic mapping study in which we study the state-of-the-art in developing software for safety-critical software for autonomous field robots. The purpose of the study is to identify practices used for the development of autonomous field robots and how these practices relate to available safety standards. Our findings from reviewing 49 papers show that standards, if at all, are barely used. The majority of the papers propose various solutions to achieve safety, and about half of the papers refer to non-standardised approaches that mainly address the methodical rather than the development level. The present study thus shows an emerging field still on the quest for suitable approaches to develop safety-critical software, awaiting appropriate standards for this support.

Keywords: Autonomous Field Robots, Safety, Standards, Development Practices, Systematic Mapping Study

1 Introduction

The domain of robotics is continuously expanding from large industrial machines in cages to free-moving consumer products. This expansion is reflected by the current market and projected increase in the future [16, 28]. Robotics is a diverse field with a variety of required skills including mechanical- and software engineering, which, due to the complexity of robotic systems, challenges researchers and practitioners [7]. For instance, mobile outdoor robots fail up to 10 times more often than other types of robots [7]. This increased risk of failure emerges from the large number of different interacting hard- and software components, e.g., control, power, communication, and sensing. All these components incorporate software, such as navigation or computer vision software, and all these components can be considered safety-critical when a robot acts autonomously. Therefore, in order to improve software quality in general


(a) Research field robot.


(b) Research field robot.


(c) Industrial field robot.

Fig. 1: Exemplarily selected field robots developed at University of Southern Denmark in different research and collaboration projects [12].

and safety-critical software in particular, different practices are applied to software development for robotic systems [1].

A subclass of mobile outdoor robots is given by *field robots*, and refers to machinery applied for outdoor tasks, e.g., in construction, forestry, and agriculture [45]. Field robots (Fig. 1) range from small research robots to large industrial agricultural robots. These robots work in a dynamically changing environment that results in challenging quality requirements regarding the software, and introduces constraints regarding perception systems, like identifying obstacles and determining the actual location [44].

Several standards aim to address the aforementioned issues to pave the way towards improved safety and quality in the respective areas by addressing hazards, functional safety, and performance alongside the development process. Despite the availability of such standards, it is still argued oftentimes that "a safe robot" is not enough and that a robot needs to be ethical for trustworthiness [43]. Nonetheless, trustworthiness of robots relies on modeling the robot as well as the environment, which is an issue notably in dynamic environments in which field robots operate.

Problem Statement Safety is considered a "hot topic" in robot development, yet missing a link to the respective standards, e.g., [2, 10, 31, 35]. Furthermore, we miss a comprehensive picture of how certification is done in practice, what (software development) practices are utilised in the development processes, and how safety is maintained in the whole ecosystem that comprises the robot and its environment.

Objective Our goal is to understand how safety-critical robot software is developed in general, and how different practices contribute to the development process—given the constraint that such a software (system) is potentially subject to certification.

Contribution In this paper, we present findings from a systematic mapping study in which we collected and structured the current body of knowledge regarding (software development) practices and standards applied to the development of safety-critical robotic software. We analysed 49 papers that were obtained in a rigorous selection procedure. Our findings show that standards are barely—if at all—used. A majority of 35 papers propose various solutions to achieve safety, and about half of the papers refer to non-standardised approaches to maintain safety, that mainly address the methodical rather than the development level. The present study thus shows an emerging field still on the quest for suitable approaches to develop and certify safety-critical software.

Outline The remainder of this paper is organised as follows: Section 2 presents the fundamentals and discusses related work. In Section 3, we present the research design, followed by the presentation and discussion of our findings in Section 4. Finally, Section 5 concludes the paper.

2 Fundamentals and Related Work

Robots depend on knowledge from many domains, which results in robotics being a multi-faceted research area. Due to the central role of software for robots, different coding practices have been tested to improve safety and quality within robotics [1]. Software quality in general and quality of robotic software in particular has received much attention over the years. From the perspective of general quality, Kitchenham et al. [23], discuss standards, quality, and their impact. Notably, considerations regarding software languages and quality have also reached the robotics domain, e.g., in control [34] and vision [15]. Issues with software quality have been reported for years, e.g., unit mismatches crashing space probes [5], overdosed drug treatments in medicine [25], and a series of problems in the automotive domain [30]. Those (representatively selected and further) problems fostered the development of safety standards. At the one end of the spectrum, recommendations based on best practices, such as MISRA [29], were developed. At the other end of the spectrum, formal standards were developed, e.g., on functional safety ISO 25119 [39] (agriculture) and ISO 26262 [38] (automotive). Such standards aim at improving the systems' quality by verifying all hazards being covered, and that the system still can be trusted when the system is malfunction.

For robotic systems in particular, some research was conducted to analyse potential hazards and how to address them appropriately, e.g., [9, 37]. Such hazard analyses usually refer to ISO 13482 [20], which is a standard for personal and mobile robots and provides a characterisation by mentioning the attributes: "multiple passengers" or "non-standing passengers" or "outdoor" or "uneven surfaces" or "not slow" or "not lightweight" or "autonomous" (ISO 13482 [20], Sect. 6.1.2.3, Person Carrier Robots, Type 3.2). The type 3.2 robot, inter alia, covers agricultural robots, mobile robots, professional and domestic service robots, and so forth—as long as the robot moves slower than 20 km/h and is not for medical, military, water-borne, or flying use. That is, the type 3.2 categorisation properly addresses autonomous field robots as well [45].

Apart from safety in general, computer vision is crucial for autonomous field robots, as it adds further requirements regarding software quality for robotic software. Computer vision is used for sensing the environment, and the standard IEC/EN 61496 [41] defines specific requirements regarding quality and functional safety of perception systems. Given the requirements regarding safe operation of robots and the complexity of sensing and recognising the operation environment, functional safety and performance have to be considered critical quality attributes. Especially performance is covered in a new upcoming standard ISO/DIS 18497 [40] that puts emphasis on quantifying the performance requirements for perception systems. However, this and other standards on functional safety only refer to human damage as a critical factor. Nevertheless, for autonomous robots, it is also of importance to detect other machines and animals to keep the robot operating.

In summary, related work on safety regarding the development of software for autonomous field robots is, in current literature, only indirectly addressed by few standards and individual studies investigating selected quality attributes. However, little is known about how software quality manifests in the software development process of robotic software. The paper at hand thus closes a gap in literature by providing a big picture and detailed information about practices used in software development and safety certification, and how available standards relate to robotic software development.

3 Research Design

In this study, we used the *Systematic Literature Review* (SLR; [22]) process to collect papers that we used in a *Systematic Mapping Study* (SMS; [32]). The core study was conducted by initially reviewing a small set of manually selected publications to form the basic knowledge (snowballing). Based on these publications, we conducted an automatic search in different literature databases to collect further publications used to perform the mapping study. The mapping study in particular aims to cover standards and development practices for robots that are autonomous, mobile, and used outdoor to address a wide range of robotics including *autonomous field robots*, *autonomous mobile robots*, and *mobile outdoor robots*.

In the subsequent sections, we detail the research method by presenting the research questions and explaining the different steps for data collection and analysis.

3.1 Research Questions

In order to investigate the state-of-the-art of safety certification practices for autonomous field robots, we formulate the following research questions:

RQ 1 *What is the current state-of-the-art of developing safety-critical software for robotic systems?* This research question aims to gather information about those (general) aspects that are considered relevant for the development of robots. Hence, this research question is purposed to lay the foundation for the development of a map of relevant topics to capture and present the entire field.

RQ 2 *What (coding) practices are used for the development of safety-critical software for robotic systems?* This research question aims at understanding the practices that are used to develop robots in safety-critical contexts. The question addresses fine-grained coding-related practices, such as code generation or code reuse, as well as methodical process-related practices, i.e., traditional or agile software development.

RQ 3 *Which certification standards are relevant for certifying software for autonomous mobile robots?* This research question aims to collect those standards that have to be considered relevant for robot development. The purpose of this question is not to only collect standards and norms relevant for autonomous field robots, but also for the domain of robot development in general (for identifying transferable knowledge).

Table 1: Reference publications used for query construction.

	Title	Subject/Contribution
[36]	Guaranteeing Functional Safety: Design for Provability and Computer-Aided Verification	certification of safety zones for vehicles and robots.
[1]	Towards Rule-Based Dynamic Safety Monitoring for Mobile Robots	domain-specific language for robot control systems.
[44]	Human detection for a robot tractor using omni-directional stereo vision	vision methods for safe operation.
[20]	ISO 13482 - The new safety standard for personal care robots	analysing ISO 13482, which also is relevant for field robots.

Table 2: Overview of the final search search queries.

	Search String
S_1	((Robot **or** Robots **or** Robotics **or** Robotic) **near** (Autonomous **or** Mobile **or** Field **or** Automated **or** Wheeled)) **and** (Safety **or** Safe) **and** (Standard **or** Standards **or** ISO **or** IEC) **and** (Perception **or** Vision **or** Software)
S_2	((Robot **or** Robots **or** Robotics **or** Robotic) **near** (Autonomous **or** Mobile **or** Field **or** Automated **or** Wheeled **or** Human) **and** (Safety **or** Safe) **and** (Perception **or** Vision **or** Software)
S_3	((Robot **or** Robots **or** Robotics **or** Robotic) **near** (Autonomous **or** Mobile **or** Field **or** Automated **or** Wheeled **or** Human)) **and** (Safety **or** Safe) **and** (ISO **or** IEC)
C_1	(Chem* **or** Surg* **or** train **or** water **or** medicin*)
Final	(S_1 **or** S_2 **or** S_3) **and not** C_1

3.2 Data Collection Procedures

The data collection procedure comprised a snowballing and an automatic search in different literature databases, and included the following steps:

- Manual selection of relevant reference publications, using snowballing.
- Construction of search strings based on the reference publications.
- Automatic search in different literature in databases.
- Definition of in-/exclusion criteria for the paper selection.

Reference Publications The study is based on a few manually selected reference publications, which are listed in Table 1. These papers served for construction of the search queries, and also served as quality assurance of the final result set as control values.

Query Construction Based on the reference publications, we iteratively constructed the search strings to query the different literature databases (Table 2). The initial search query construction resulted in S_1, however, to achieve a larger margin of perception and results in relation to safety and safety standards with human interactions, the additional alterations were created. The context selector C_1 was created to remove results from areas that were not fitting with the overall objective of the study. Each database was queried thrice and utilising C_1 in all searches. The queries from Table 2 were used to

Table 3: Inclusion and exclusion criteria for the study.

No.	Description
IC_1	Title, keyword list or abstract make it explicit that the paper is related to safety in field robotics.
IC_2	The paper is on tools, procedures or development methods.
IC_3	The paper is in a journal, proceedings, conference or magazine (Special case for Springer Link to include chapters).
IC_4	The paper describes a long term observation of the use of development methods in relation to safety-critical development.
IC_5	The paper surveys practitioners for the use of development methods.
IC_6	The paper reports on the use of development methods in general, e.g., as secondary study.
IC_7	The paper is on tools implementing certain methods (infer information about method use), for development of safety-critical software.
IC_8	The paper describes the use of perception and sensor information for safe operation (e.g., navigation, control, obstacle avoidance etc.).
IC_9	The paper is about important aspects for environment sensing (e.g., transversal of rough terrain, stability monitoring, etc.).
EC_1	The paper is a proposal only.
EC_2	The paper is not within safety or field robotics.
EC_3	The paper occurred multiple times in the result set.
EC_4	The paper is a workshop-, tutorial-, Ph.D. summary or poster summary.
EC_5	The paper does not touch the domain of software engineering, computer science or robotics in general.
EC_6	The paper is not in English.
EC_7	The paper's full text is not available for download.

search the following databases[1], which have a certain focus on software development: *ACM Digital Library*, *SpringerLink*, *IEEE Digital Library* (XPlore), *Wiley InterScience*, and *ScienceDirect* (Elsevier). As the initially conducted test runs delivered a large number of hits and a considerable overhead, we decided to only include the top-50 results per search, which results in a maximum of 150 hits per database (cf. Table 6).

3.3 Analysis Procedures

In this section, we describe the analysis preparation steps and the procedures used for the in-depth analysis of the final result set.

Analysis Preparation To prepare the data analysis, we applied a proven procedure (cf. [24]) in which we (1) harmonised the result set by merging the individual search results and by removing the multiple occurrences, and (2) conducted a multi-staged

[1] **Note:** For technical reasons, we decided to define multiple search queries. For example, Wiley did not have the NEAR operator which was changed to and AND. ScienceDirect used W/n instead of the NEAR operator. IEEE had limitations on the search string length resulting in the asterisk (*) was used, further the NEAR operator could not be used if an asterisk was used resulting in NEAR was changed to an AND operator. In addition S_1 in connection with C_1 was too long, resulting in only surg* and medicin* from C_1 was used.

Table 4: Categories to capture development practices used in software development.

Criterion	Description
Simulation	Code or application is tested/proven using simulation.
Formal Implementation Verification	System/code is described using a formal language that facilitates analysis, to guarantee/prove system properties.
Mathematical Modeling and Algorithms	Using mathematics to prove/guarantee system properties.
Behaviour Modeling	System models, Fault tolerant models and decision theory, e.g. to make diagnosis of systems and/or reconfiguration of the system.
Formal Specification Deriving Implementation	Based on formal specification, e.g. Domain Specific Language (DSL), utilising code generation for implementation.
Misc	Papers that either encompasses many of the above methods, or do not clearly define which method is used.
Not in Software Development	Papers that does not focus on software or development practices.

Table 5: Categories to capture standards used in safety-critical software development.

Criterion	Description
IEC 61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES).
ISO 13482	limited primarily to human care related hazards but, where appropriate, it includes domestic animals or property.
ISO 26262	Road vehicles Functional safety.
ISO 10218	Robots and robotic devices Safety requirements for industrial robots.
IEC 61499	open standard for distributed control and automation.
Guaranteeing safety	Not necessarily using a standard approach.
Non-Standard Approach	When it is specifically mentioned that there is no standards available for the domain.

voting procedure. In the voting procedure, two researchers performed an independent voting. The relevance of a paper was determined by applying the in-/exclusion criteria from Table 3. Based on the publication's title and abstract, each researcher voted a paper "in" (value 1) or "out" (value 0). If both researchers agreed, a paper was in the final result set (2 points), or a paper was excluded from further investigation (0 points). For those papers that were not finally decided in this stage, a third reviewer was called in to provide his votes and to make the final decision.

In-depth Analysis Having prepared the result set, we conducted the in-depth analysis to answer the research questions. In the following, we describe the applied procedures and link them to the research questions.

Schema Construction Following the steps of conducting a systematic mapping study [32], as a first step, we select standard classification schemas to provide an overview

of the publications, and develop study-specific classification schemas from the result set. As standard classification schemas, we opt for the the *research type facet* and the *contribution type facet* as used by Wieringa et al. [42] and Petersen et al. [32]. These standard schemas are mainly used to answer RQ_1 and to draw a big picture of the maturity and the contributions provided by the studied result set.

Specific to the study, we developed further schemas, notably, to address RQ_2 and RQ_3. Table 4 presents the classification schema that was used to categorise the publications according the practices used in the software development (RQ_2). In particular, based on the different aspects of software development, we included methodical as well as technical practices, such as formal specification or simulation. In order to answer RQ_3, we collected information about norms and standards used in safety-critical systems. Table 5 presents the respective categories, but respects situations in which standards are not applied or available.

Data Presentation To present the data, we visualise our data using systematic maps. Furthermore and due to the limited number of papers in the result set, we only use simple tables and charts to provide the data and a (tentative) interpretation of the results.

3.4 Validity Procedures

To increase the validity of our study, we apply different techniques. Prior to the actual study, we analyse the domain of interest and select few reference publications, which are used to develop the search queries for the automated search. The developed search queries were tested in several dry-runs, and iteratively refined. To overcome subjectivity in the study selection, the study selection process is based on a proven procedure that relies on multi-staged voting procedures and researcher triangulation [24]. Furthermore, the classification of the result set is performed using standardised classification schemas [32,42]. The study-specific schemas were either grounded in standard schemas or crafted from common/observed terms and practices in the found publications.

4 Study Results

In this section, we present and discuss the results of the study. We provide an overview of the study population in Section 4.1, before answering the research questions in Sections 4.2 – 4.4. Finally, we briefly discuss our findings and provide a (tentative) interpretation in Section 4.5.

4.1 Study Population

Table 6 provides an overview of the number of publications obtained from the different search steps. The initial search resulted in more than 63,000 hits. After applying the different in-/exclusion criteria (Table 3), eventually, 49 papers were selected for further investigation.

Table 6: Overview of the publication numbers obtained from the literature search (per database, per data collection step, cf. Section 3.2 and 3.3).

Step	**IEEE**	**ACM**	**Springer**	**Elsevier**	**Wiley**	**Total**
Step 1: Search						
(S_1 **OR** S_2 **OR** S_3)	1,298	2,892	15,509	37,114	6,585	63,398
Step 2: Filtering						
Apply F_1 and limit on results set (50)	150	88	150	149	150	687
Remove duplicates	42	0	42	46	43	187
Result Set (before the voting):	80	107	108	104	101	500
Final result set	10	2	26	8	3	**49**

Figure 2 visualises the result set according to the publication frequency over time (the result set contains publications from 1987 to 2015). Furthermore, the figure includes the classification according to the research type facets to illustrate the development of the considered domain over time.

From this information, we see safety-critical software development for autonomous field robots being a still emerging discipline, which gained more interest in the early 2000's. Since then, we observe the majority of the published papers of type *solution proposal* (35 out of 49), complemented by a few papers of type *evaluation research* (4 out of 49). However, in the result set, we find only seven papers of type *philosophical*, which indicates a gap of structuring/synthesising research activities, such as literature studies.

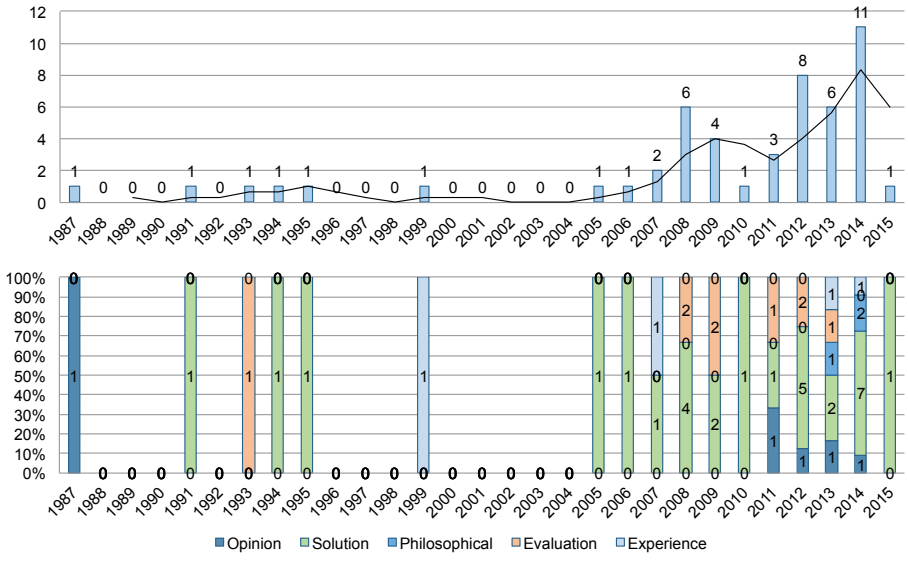

Fig. 2: Number of papers per year and distribution over the research type facets.

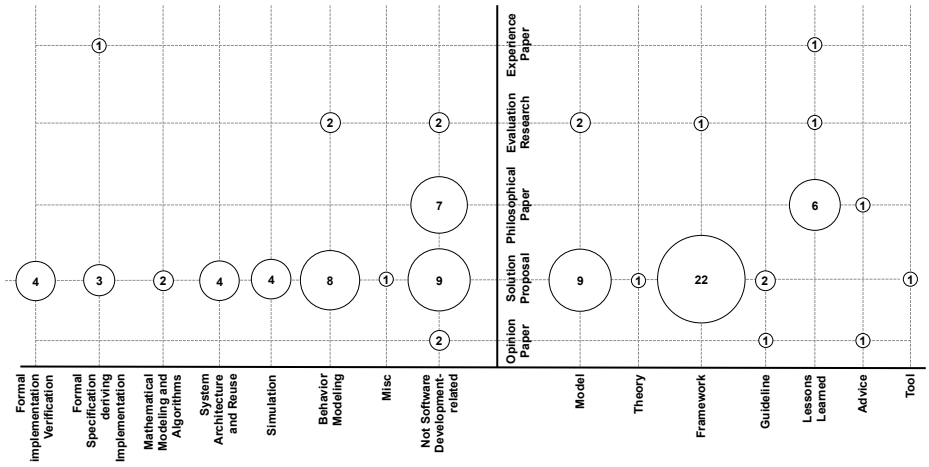

Fig. 3: Systematic map illustrating research type facets, contribution type facets, and software development practices.

4.2 RQ 1: State-of-the-art of Developing Safety-critical Robotic Software

To present the state-of-the-art and the practices used for development (Sect. 4.3), we provide an integrated systematic map (Fig. 3). The right part of Fig. 3 illustrates the research- and contribution type facets and shows the majority of the papers proposing models (9 out of 49) or frameworks (22 out of 49). That is, the current publication body is focused on proposing new approaches to deal with the challenges coming along with developing safety-critical software for autonomous field robots. However, the map also shows eight papers presenting lessons learned. Nonetheless, the map clearly points to an emerging field.

Key-wording the abstracts of the selected papers reveals the focus points of these studies. Here, the focus lays on mobile and autonomous robots, and emphasis is put on software/system development (in general), control, environment, interaction with humans, modeling, and standards. Among all selected publications, the term “standards” was mentioned 32 times in the abstracts, also indicating the increasing interest in standards supporting the development of safe and performant robotic software.

4.3 RQ 2: Practices for the Development of Safety-critical Robotic Software

The left part of Fig. 3 provides an overview of the publication classification regarding the practices applied to the development of safe robotic software (Table 4). The chart shows that, given that the majority of the papers is categorised as *solution proposal*, many different aspects are covered and that many different practices are addressed. However, regarding those practices that are close to software development, formal verification, software architecture and reuse, simulation, and behaviour modeling are the flourishing areas.

Nevertheless, 20 papers are categorised into the non-development-related practices, which, among other things, include development approaches/methods, best practices

Simulation	Formal implementation verification	Mathematical modeling and algorithms	System architecture and reuse	Misc	Behavior modeling	Formal specification deriving implementation	Not SW dev-related	
0	1	1	1	0	0	1	1	IEC 61508
0	0	0	1	0	0	0	2	ISO 13482
0	0	0	0	1	0	0	0	ISO 26262
0	0	0	0	0	0	0	0	ISO 10218
0	0	0	0	0	0	1	0	IEC 61499
0	3	2	0	0	1	0	2	Guranteeing safety - Not necessarily using a Standard approach
4	1	0	2	1	9	2	15	Non-Standard Approach
0	0	0	0	0	0	1	0	No standards available

Fig. 4: Heat-map on the connection of standards with development practices.

regarding the way to develop software, or standards to be applied in the development. Therefore, the map indicates this research field still investigating different ways of obtaining safe field robots, with a slight trend towards modeling the robot as such and its environment. However, the map also raises the question for the maturity of the development approach and the underlying theories. For instance, only five papers deal with formal specification, mathematical models, and algorithms, while the majority of the development-related practices looks for modeling, design, and simulation. From the available data, we cannot conclude whether or not the theoretical parts are already in place. Furthermore, the studied papers do not allow for concluding to what extent those practices that improve software reliability are adopted for the development of robotic software. So far, we can only conclude that—at least for the development-related practices—the community is on the quest for pragmatic approaches to design and develop safe robotics software.

4.4 RQ 3: Certification Standards for Robotic Software

The third research question aims at investigating the role currently available standards for safety play in the development of software for autonomous field robots. Therefore, we collected the major standards addressing this topic for general software development as well as for related/specialised domains (cf. Table 5). Due to the scarcely available studies explicitly investigating the use and impact of standards in domain under consideration and due to the observation that available papers usually refer to multiple standards, we decided against creating a systematic map. Instead, we provide a heat-map in Fig. 4 to visualise the connections between the standards and the development practices (Table 4).

The heat-map shows—if at all—an only loose connection between development practices and available standards. Only the IEC 61508 (general functional safety) was mentioned in connection to different practices. However, the figure shows that safety seems to be mainly addressed by non-standardised approaches. At the same time, safety is aimed to be achieved by not-development-related practices, i.e., at the level of methods and approaches to develop the software/system. Although closely related to au-

tonomous field robots, the standard ISO 10218 (industrial robots) was not referred at all. The overall picture drawn by the heat-map, however, shows a low involvement of standards in the robotic software development.

4.5 Discussion & Interpretation

Our findings indicate a trend toward developing new methods and processes to facilitate development of safety-critical robots (Fig. 2). Nevertheless, the current utilisation of standards is very limited (Fig. 4), and non-standardised approaches are used to ensure safety. So far, our findings present a snapshot and a baseline, as a new standard that explicitly addresses field robots ISO 13482 was recently released (September 2014); this standard is already mentioned thrice by independent studies [13, 19, 20]. That is, although we could not obtain much information on the use of standards in robot software development now, we expect an increasing number of projects and companies utilising this standard, an increasing number of studies and, thus, more evidence regarding the standard's suitability in future. This observation is also supported by an article in which authors specifically stated that they were missing a standard for their development [4], which should be available now.

RQ_2 uncovered that the majority of the results were solution proposals focusing on behaviour modeling, with a lower focus on reliable software development (categories: formal implementation verification [3, 8, 11, 33], formal specification deriving implementation [1, 4, 14, 26], and mathematical modeling and algorithms [6, 27]). From our perspective these categories would give the highest confidence in safety-critical software. The limited use of these categories within robotic software development puts high constraints on the certification authorities, because the assessors need to be methodical and stringent when manually evaluating the code.

This issue is increased in magnitude when computer vision is introduced. As mentioned before, field robots have to sense and react to a dynamically changing environment. Looking into those papers dealing with computer vision, our findings show the main focus of vision-related software development instrumenting the *Non-standard approach* (Fig. 4) to provide safety. We also found these papers having a very limited use of formal methods or guarantees to uphold the safety in the vision system. This knowledge uncovers that within field robotics, guaranteeing safety in relation to perception and software by using certification is an area that has been neglected. Looking at vision in connection with the research type facet categorisation, it shows that the vision papers are solution driven, as was also the case for software.

5 Conclusion

This study presents the findings from a systematic mapping study on the use of safety certification practices in autonomous field robot software development. In a rigorous search and selection procedure, 49 papers were considered for investigation.

Our findings show the majority of the papers proposing new solutions addressing various aspects of safety and related software development practices. However, available standards are neglected, and more than a half of the papers shows non-standardised

approaches used to develop safe robots. Nevertheless the limited use of standards limits the credibility of the achieved safety, and limits the usability.

A reason could be the relatively fresh standard ISO 13482 for this domain. Nonetheless, the minimal use of formal specification and verification in combination with guaranteeing safety might point to a significant focus on solution approaches for an emerging field thus not yet facing the need to fulfil stringent requirements by standards. For this, improved tool support could help researchers to facilitate the use of standards for safety-critical robotic software.

Finally, the domain of field robotics has been primarily focused on solutions. The absence of secondary studies shows a need for more research to structure and uncover the best way of achieving safe autonomous field robots. Furthermore, although standards were contributed to the community, those are neglected to a large extent. The community thus needs to foster a critical discourse on the availability and appropriateness of the available standards and complementing support tools, and to work out actionable approaches, as for instance proposed in [17, 18].

Threats to Validity & Limitations As a literature study, this study suffers from potential incompleteness of the search results and a general publication bias, i.e., positive results are more likely published than failed attempts. That is, our study encounters the risk to draw an incomplete and potentially too positive picture. Beyond that general threat, the validity of the study could be biased by personal ratings of the participating researchers. To address this risk, we relied on a proven procedure [24] that utilises different supporting tools and researcher triangulation to support dataset cleaning, study selection, and classification. Another threat to validity is the study selection as such. As we faced a fairly unstructured domain for which no other structuring secondary studies are available, we had to iteratively develop and test the search queries. Furthermore, due to the terminology that suffers heterogeneity and massive overloading, e.g., the term "Standard" or (potentially) different meanings of the studied concepts like "Simulation", we received more than 63,000 hits, and we decided to limit the number of hits to be considered for the investigation to 50 (max.) per query run. Although we found this approach sufficient in previously conducted studies, such as [21], the final result set investigated in the present study needs to be considered with care, as we have no knowledge about publications not triggered by the search and selection procedures applied in this study.

Our contribution aims at creating a big picture of the research field thus having some limitations. Deeper insights and analyses regarding conceptual, methodical, and technical aspects of safety-certification practices are not part of this study. Furthermore, our study does not aim at creating taxonomies or generalised concepts. However, we could provide the basis to support such next steps and further discussion.

Future Work The present study is a first step toward a deeper understanding of safety certification in autonomous field robot development. In this instance of the study, we primarily looked for "robots", but, in future, need to extend our work to "Automated Ground Vehicles (AGV)" to provide a more comprehensive picture and to develop appropriate process improvement proposals. Furthermore, standards in general and those mentioned in Table 5 have to be revisited to improve understanding about their relevance within the investigated domain. Given the domain's requirements, in-depth in-

vestigation, e.g., of IEC 61508 and other relevant standards, and the relation to development practices is necessary. That is, it is crucial to understand whether coding practices can be evaluated homogeneously across the standards or if an evaluation of those standards against the MISRA [29] software guidelines better contributes to the general understanding.

A second important facet is the extension of our study: So far, due to absence of respective structuring studies, our purpose was to initially generate a big picture of the domain. That is, the present study provides an overview and an initial domain structure proposal, which is grounded in reviewing scientific literature only. Continuing, the study needs to be refined and updated, e.g., by improving the search queries and classification schemes. Furthermore, practitioners need to be surveyed to (1) bring more practically relevant problems and experience into the study, to (2) confirm our tentative findings, and (3) to improve the data quality thus allowing for steering future research, such as supporting certification process improvement, improvement of (agile) software development in regulated environments, or to support tool development. This also helps improving the situation that notably many SMEs face: the push for showing new solutions limits the applicability of standards, because they are large and cumbersome to work with. For example, a formal specification tool for vision pipelines, such as proposed by Hochgeschwender et al. [15] and our recent contributions [17, 18] focusing on safety and how to improve the development within computer vision, as is for example seen within control of robotics [1, 3, 4, 8, 26]. Providing a formal specification tool for safety-critical vision applications would greatly improve the possibility of complying with ISO 13482.

References

1. S. Adam, M. Larsen, K. Jensen, and U. P. Schultz. Towards rule-based dynamic safety monitoring for mobile robots. In *Simulation, Modeling, and Programming for Autonomous Robots*, number 8810 in Lecture Notes in Computer Science, pages 207–218. Springer, 2014.
2. P. Biber, U. Weiss, M. Dorna, and A. Albert. Navigation system of the autonomous agricultural robot Bonirob. In *Workshop on Agricultural Robotics: Enabling Safe, Efficient, and Affordable Robots for Food Production*, 2012.
3. G. Biggs, K. Fujiwara, and K. Anada. Modelling and analysis of a redundant mobile robot architecture using aadl. In *Simulation, Modeling, and Programming for Autonomous Robots*, volume 8810 of *Lecture Notes in Computer Science*, pages 146–157. Springer, 2014.
4. G. Biggs, T. Sakamoto, K. Fujiwara, and K. Anada. Experiences with model-centred design methods and tools in safe robotics. In *International Conference on Intelligent Robots and Systems*, pages 3915–3922. IEEE, 2013.
5. M. I. Board. *Mars Climate Orbiter Mishap Investigation Board Phase I Report November 10, 1999*. 1999.
6. S. Bouraine, T. Fraichard, and H. Salhi. Provably safe navigation for mobile robots with limited field-of-views in dynamic environments. *Autonomous Robots*, 32(3):267–283, 2012.
7. J. Carlson, R. R. Murphy, and A. Nelson. Follow-up analysis of mobile robot failures. In *IEEE International Conference on Robotics and Automation*, volume 5, pages 4987–4994. IEEE, 2004.
8. L. de Silva, R. Yan, F. Ingrand, R. Alami, and S. Bensalem. A verifiable and correct-by-construction controller for robots in human environments. In *International Conference on Human-Robot Interaction Extended Abstracts*, pages 281–281. ACM, 2015.

9. S. Dogramadzi, M. E. Giannaccini, C. Harper, M. Sobhani, R. Woodman, and J. Choung. Environmental hazard analysis - a variant of preliminary hazard analysis for autonomous mobile robots. *Journal of Intelligent & Robotic Systems*, 76(1):73–117, 2014.
10. L. Emmi, M. Gonzalez-de Soto, G. Pajares, and P. Gonzalez-de Santos. New trends in robotics for agriculture: Integration and assessment of a real fleet of robots. *The Scientific World Journal*, 2014:1–21, 2014.
11. U. Frese, D. Hausmann, C. Lüth, H. Täubig, and D. Walter. The importance of being formal. *Electronic Notes in Theoretical Computer Science*, 238(4):57 – 70, 2009.
12. Frobomind. `http://www.frobomind.org`.
13. V. Gribov and H. Voos. Safety oriented software engineering process for autonomous robots. In *Conference on Emerging Technologies & Factory Automation*, pages 1–8. IEEE, 2013.
14. R. Hanai, H. Saito, Y. Nakabo, K. Fujiwara, T. Ogure, D. Mizuguchi, K. Homma, and K. Ohba. RT-component based integration for IEC 61508 ready system using SysML and IEC 61499 function blocks. In *IEEE/SICE International Symposium on System Integration*, pages 105–110. IEEE, 2012.
15. N. Hochgeschwender, S. Schneider, H. Voos, and G. K. Kraetzschmar. Declarative Specification of Robot Perception Architectures. In *Simulation, Modeling, and Programming for Autonomous Robots*, pages 291–302. Springer, 2014.
16. IFR. World Robotics 2014 Industrial Robots, 2014.
17. J. T. M. Ingibergsson, U. P. Schultz, and D. Kraft. Towards declarative safety rules for perception specification architectures. In *International Workshop on Domain-Specific Languages and models for ROBotic systems (DSLRob-15)*, (in press) 2015.
18. J. T. M. Ingibergsson, S.-D. Suvei, M. K. Hansen, P. Christiansen, and U. P. Schultz. Towards a DSL for perception-based safety systems. In *International Workshop on Domain-Specific Languages and models for ROBotic systems (DSLRob-15)*, (in press) 2015.
19. T. Jacobs, U. Reiser, M. Haegele, and A. Verl. Development of validation methods for the safety of mobile service robots with manipulator. In *German Conference on Robotics (ROBOTIK 2012)*, pages 1–5. VDE-Verl., 2012.
20. T. Jacobs and G. S. Virk. ISO 13482 – the new safety standard for personal care robots. In *International Symposium on Robotics (ROBOTIK 2014)*, pages 1–6. VDE-Verl., 2014.
21. G. Kalus and M. Kuhrmann. Criteria for software process tailoring: a systematic review. In *Proceedings of the 2013 International Conference on Software and System Process*, pages 171–180. ACM, 2013.
22. B. Kitchenham. Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33(2004):1–26, 2004.
23. B. Kitchenham and S. L. Pfleeger. Software Quality: The Elusive Target. *IEEE software*, 13(1):12–21, 1996.
24. M. Kuhrmann, D. M. Fernández, and M. Tiessler. A mapping study on the feasibility of method engineering. *Journal of Software: Evolution and Process*, 26(12):1053–1073, 2014.
25. N. Leveson and C. Turner. An investigation of the Therac-25 accidents. *Computer*, 26(7):18–41, July 1993.
26. M. Machin, F. Dufossé, J.-P. Blanquart, J. Guiochet, D. Powell, and H. Waeselynck. Specifying safety monitors for autonomous systems using model-checking. In *Computer Safety, Reliability, and Security*, volume 8666 of *Lecture Notes in Computer Science*, pages 262–277. Springer, 2014.
27. E. Masehian and Y. Katebi. Sensor-based motion planning of wheeled mobile robots in unknown dynamic environments. *Journal of Intelligent & Robotic Systems*, 74(3-4):893–914, 2014.
28. METI. Trends in the Market for the Robot Industry in 2012, July 2013.
29. MISRA. MISRA-C Guidelines for the Use of the C Language in Critical Systems, 2012.

30. R. L. Mitchell. Toyota's lesson: Software can be unsafe at any speed, Feb. 2010.
31. S. J. Moorehead, M. Kise, and J. F. Reid. Autonomous Tractors for Citrus Grove Operations. In *International Conference on Machine Control & Guidance*, pages 309–313, 2010.
32. K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson. Systematic mapping studies in software engineering. In *International Conference on Evaluation and Assessment in Software Engineering*, pages 68–77. British Computer Society, 2008.
33. M. Rahimi and X. Xiadong. A framework for software safety verification of industrial robot operations. *Computers & Industrial Engineering*, 20(2):279 – 287, 1991.
34. M. Reichardt, T. Föhst, and K. Berns. On software quality-motivated design of a real-time framework for complex robot control systems. In *International Workshop on Software Quality and Maintainability*, 2013.
35. F. Rovira-Más. Sensor architecture and task classification for agricultural vehicles and environments. *Sensors*, 10(12):11226–11247, 2010.
36. H. Täubig, U. Frese, C. Hertzberg, C. Lüth, S. Mohr, E. Vorobev, and D. Walter. Guaranteeing functional safety: design for provability and computer-aided verification. *Autonomous Robots*, 32(3):303–331, Apr. 2012.
37. TC 184. Robots and robotic devices - Safety requirements for personal care robots. International Standard ISO 13482:2014, International Organization for Standardization, 2014.
38. TC 22. Road Vehicles Functional Safety. International Standard ISO 26262:2011, International Organization for Standardization, 2011.
39. TC 23. Tractors and machinery for agriculture and forestry – safety-related parts of control systems. International Standard ISO 25119-2010, International Organization for Standardization, 2010.
40. TC 23. Agricultural machinery and tractors – Safety of highly automated machinery. International Standard ISO/DIS 18497, International Organization for Standardization, 2014.
41. TC 44. Safety of machinery – electro-sensitive protective equipment. International Standard IEC 61496-2012, International Electronical Commission, 2012.
42. R. Wieringa, N. Maiden, N. Mead, and C. Rolland. Requirements engineering paper classification and evaluation criteria: a proposal and a discussion. *Requirements Engineering*, 11(1):102–107, 2006.
43. A. Winfield, C. Blum, and W. Liu. Towards an ethical robot: Internal models, consequences and ethical action Selection. In *Advances in Autonomous Robotics Systems*, volume 8717 of *Lecture Notes in Computer Science*, pages 85–96. Springer, 2014.
44. L. Yang and N. Noguchi. Human detection for a robot tractor using omni-directional stereo vision. *Computers and Electronics in Agriculture*, 89:116–125, 2012.
45. S.-Y. Yang, S.-M. Jin, and S.-K. Kwon. Remote control system of industrial field robot. In *IEEE International Conference on Industrial Informatics*, pages 442–447. IEEE, 2008.