A Systematic Analysis of Functional Safety Certification Practices in Industrial Robot Software Development

Xie Tong[1,*] and Wu Lei[2]

[1]School of Software, Beijing Institute of Technology, Beijing, China
[2]Software Quality Engineering Research Centre, The Fifth Electronic Research Institute of MIIT, Guangzhou, China
Corresponding Email: vickyxt@163.com

Abstract. For decades, industry robotics have delivered on the promise of speed, efficiency and productivity. The last several years have seen a sharp resurgence in the orders of industrial robots in China, and the areas addressed within industrial robotics has extended into safety-critical domains. However, safety standards have not yet been implemented widely in academia and engineering applications, particularly in robot software development. This paper presents a systematic analysis of functional safety certification practices in software development for the safety-critical software of industrial robots, to identify the safety certification practices used for the development of industrial robots in China and how these practices comply with the safety standard requirements. Reviewing from Chinese academic papers, our research shows that safety standards are barely used in software development of industrial robot. The majority of the papers propose various solutions to achieve safety, but only about two thirds of the papers refer to non-standardized approaches that mainly address the systematic level rather than the software development level. In addition, our research shows that with the development of artificial intelligent, an emerging field is still on the quest for standardized and suitable approaches to develop safety-critical software.

1 Introduction

Industrial robot, as defined by ISO 8373 [1]: An automatically controlled, reprogrammable, multipurpose manipulator programmable in three or more axes, which may be either fixed in place or mobile for use in industrial automation applications. An automatically controlled, reprogrammable, multipurpose manipulator programmable in three or more axes, which may be either fixed in place or mobile for use in industrial automation applications. The main customer for industrial robots - the automotive industry - is changing and diminishing. There is a worldwide trend towards automation in the 'non-automotive industry'. Robot suppliers are offering increasingly tailored solutions to customers in China, as the "Made in China 2025" plan which focus on the development of fully-automated "smart" factories has a strong support from the government.

As the industrial robots becoming smarter, faster and cheaper, they're being called upon to do more. They're taking on more "human" capabilities and traits such as sensing, dexterity, memory and trainability. As a result, they're taking on more jobs - such as picking and packaging, testing or inspecting products, or assembling minute electronics. Also, a new generation of "collaborative" robots (Figure 1) ushers in an era of shepherding robots out of their cages and the robots work literally hand-in-hand with human workers who train them through physical demonstration.

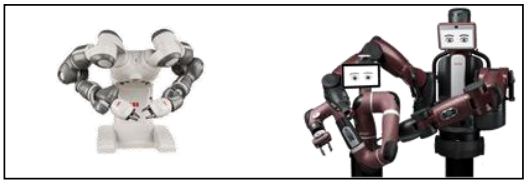

Fig. 1. A new generation of "collaborative" robots by ABB (left) and Rethink Robotics (right).

The power and size of industrial robots means that they are capable of inflicting severe injury if programmed incorrectly or used in an unsafe manner. Due to the mass, high-speeds and the new "collaborative" behavior of

industrial robots, it is always unsafe for a human to remain in the work area of the robot during automatic operation. The system can begin motion at unexpected times and a human will be unable to react quickly enough in many situations, even if prepared to do so. Thus, great care must be taken to make an industrial robot safe for human workers or human interaction.

Programming errors represent a serious safety consideration, particularly in large industrial robots. Those problem prompted the development of software safety standards, such as recommendations based on best practices (MISRA [2]), and formal standards(ISO 25119 [3] for agriculture and ISO 26262 for automotive [4]). For robotic systems, there are some researches analyze potential hazards [5,6] refer to ISO 13482 [7], which is aimed to achieve safety requirements not for industrial robots but for personal care robots. ISO 10218 [8] is conducted to recognize the particular hazards which are presented by industrial robots and industrial robot systems. Regarding the development of software for industrial robots, those related safety research can only be addressed by few standards indirectly. Moreover, those standards or studies gave the requirements only, but didn't provide the guidance of how to implement.

In summary, we present findings from a systematic review in which we collected and structured from the current body of knowledge regarding (software development) practices and standards applied to the development of safety-critical robotic software in China. Our research from reviewing academic papers written in Chinese, shows that safety standards are barely used in software development of industrial robot in domestic.

A systematic literature review is a means of identifying, evaluating and interpreting all available research relevant to a particular research question, or topic area, or phenomenon of interest. There are three existing guidelines for systematic reviews [9-11], but all these guidelines are intended to aid medical researchers. In particular, software engineering research has relatively little empirical research compared with the large quantities of research available on medical issues. This article aims to analysis the functional safety certification practices in industrial robot software development, following a guideline for systematic reviews which is appropriate for software engineering researchers proposed by Barbara Kichenham [12].

2 Review questions

We formulate the following research questions:

RQ1: what standards or certifications for industrial robot software development have been adopted in domestic? This research questions aims to investigate the current states of standards for software development.

RQ2: What practices are used for the development of safety-critical software for industrial robotic systems (including coding and testing)? This research question aims at understanding the practices that are used to develop robots in safety-critical contexts. The question addresses coding and testing practices, such as code generation or code reuse, unit testing or fault injection and so on.

RQ3: Which certification standards have provided feasible implementation guidelines for software for industrial robots? This research question aims to find out whether the current standards are suitable for implement and test safety-critical software for industrial robots.

3 Review methods

3.1 Data sources and search strategy

The process of performing a systematic review must be transparent and replicable. We constructed the search strings (Table1) based on ISO 10218-2011 [8].

Table 1. Overview of the final search queries.

	Search queries (searching scope: FT-full-text; AB-abstract)
S1	1. (FT="Robot" OR FT="Robots") AND (FT="Industry" OR FT="Industrial") AND (FT="Safety" OR FT="safe") AND (FT="Standard" OR FT="Standards" OR FT="ISO" OR FT="IEC" OR FT="GB") AND (FT="Software" OR FT="test" OR FT="testing") 2. (AB="Robot" OR AB="Robots") AND (AB="Industry" OR AB="Industrial") AND (AB="Safety" OR AB="safe") AND (AB="Standard" OR AB="Standards" OR AB="ISO" OR AB="IEC" OR AB="GB") AND (AB="Software" OR AB="test" OR AB="testing"

S2	1. (FT="Robot" OR FT="Robots") AND (FT="Industry" OR FT="Industrial") AND (FT="Safety" OR FT="safe") AND (FT="Standard" OR FT="Standards" OR FT="ISO" OR FT="IEC" OR FT="GB") 2. (AB="Robot" OR AB="Robots") AND (AB="Industry" OR AB="Industrial") AND (AB="Safety" OR AB="safe") AND (AB="Standard" OR AB="Standards" OR AB="ISO" OR AB="IEC" OR AB="GB")
S3	1. (FT="Robot" OR FT="Robots") AND (FT="Industry" OR FT="Industrial") AND (FT="Safety" OR FT="safe") AND (FT="Software" OR FT="test" OR FT="testing") 2. (AB="Robot" OR AB="Robots") AND (AB="Industry" OR AB="Industrial") AND (AB="Safety" OR AB="safe") AND (AB="Software" OR AB="test" OR AB="testing")
C1	(AB="medicin*" OR AB ="surgence*" OR AB ="health-care")
Final	(S1 OR S2 OR S3) AND NOT C1

In order to assure the accuracy and universality of the searching results, we used the following databases for querying (Table 2). The databases are the largest and continuously updated Chinese database in the world, including journals, doctoral dissertations and masters' theses full-text databases, which have a certain focus on software development.

Table 2. Databases used for searching.

Name of database	Search strategy for each database	Date of search	Years covered by search
China Academic Journals Full-text Database (CJFD)	(S1 or S2 or S3) and not C1	2016.5	1984-Now
China Doctoral Dissertations Full-text Database (CDFD)	(S1 or S2 or S3) and not C1	2016.5	1984-Now
China Masters' Theses Full-text Database (CMFD)	(S1 or S2 or S3) and not C1	2016.5	1984-Now

3.2 Study selection

Intended to identify these primary searches that provide direct evidence about our research questions, according to the questions from chapter 3, inclusion and exclusion criteria are defined as follow:

3.2.1 Inclusion criteria

• Title, keyword list or abstract make it explicit that the paper is related to safety in industrial robotics;

• The paper is on tools, procedures or development methods;
• The paper is in a journal, proceedings, magazine, doctoral dissertations or masters' theses;
• The paper describes a long term observation of the use of development methods in relation to safety-critical development;
• The paper surveys practitioners for the use of development methods;
• The paper is on tools implementing certain methods (infer information about method use), for development of safety-critical software;
• The paper is about important aspects for industrial networking, industrial control safety.

3.2.2 Exclusion criteria

• The paper is a proposal only;
• The paper is not within safety or industrial robotics;
• The paper occurred multiple times in the result set;
• The paper does not touch the domain of software engineering, computer science or robotics in general;
• The paper's full text is not available for download.

3.3 Data extraction

The objective of data extraction is to design data extraction forms to accurately record the information which are obtained from the primary studies by researchers. The data extraction forms (Table 3 & Table 4) were designed to collect all the information needed to address the review questions and the study quality criteria. Following the steps of conducting a systematic mapping study [13], we developed schemas to address RQ1, RQ2 and RQ3. Table 3 presents the classification schema that was used to classify the publications according to the practices used in the software development (RQ2). In particular, based on the different aspects of software development, we included software design, implement, and testing practices, such as formal specification, fault injection, simulation. In order to answer RQ3, we collected information about norms and standards used in safety-critical systems (Table 4).

Table 3. Development practices in software development (including software design, implement and testing).

Aspects	Practices
Architectural design	Notations for architectural design (Semi-formal notations, formal notations, etc.)
	Error detection at the software architectural level (Range checks, plausibility check, control flow monitoring, diverse software design, etc.)
	Error handling at the software architectural level (Static recovery mechanism, graceful degradation, independent parallel redundancy, correcting codes for data, etc.)
	Verification of the software architectural design (Walk-trough, inspection, simulation, prototype generation, formal verification, control flow analysis, data flow analysis, etc.)
Unit design and implementation	Notations for software unit design (Natural language, semi-formal notations, formal notations, etc.)
	Verification of software unit design and implementation (Walk-trough, inspection, semi-formal and formal verification, control flow analysis, data flow analysis, static code analysis, semantic code analysis, etc.)
testing	Methods for software testing (requirements-based test, interface test, fault injection test, resource usage test, back-to-back comparison test between

	model and code, etc.)
	Methods for deriving test cases for software testing (analysis of requirements, generation and analysis of equivalence classes, analysis of boundary values, error guessing, etc.)
	Structural coverage metrics at the testing level (statement coverage, branch coverage, modified condition/decision coverage)
Others	Misc (papers that either encompasses many of the above methods, or do not clearly define which method is used)
	Not in Software Development

Table 4. Standards used in safety-critical software development.

Standards	Description
ISO 10218	Robots and robotic devices Safety requirements for industrial robots (IDT by GB 11291-2013)
IEC 62061	Electrical safety of machinery—Functional safety of safety-related electrical electronic and programmable electronic control systems (IDT by GB 28526-2012)
IEC 61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES) (IDT by GB/T 20438-2007)
IEC 61131-6-2012	Programmable controllers -- Part 6: Functional safety (IDT by GB/T 15969-2007)
IEC 61511-2003	Functional safety - Safety instrumented systems for the process industry sector (GB/T21109-2007)
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 are no standards available for the domain

3.4 Data synthesis & analyze

In this section, we present the results of the included primary studies using data synthesis and analyze. In Sect.4.4.1, we give an overview of the research. In Sect.4.4.2 – Sect.4.4.4, we answer the research questions.

3.4.1 General overview

An overview of results obtained from the different search steps are provided as Table 5. Step1, we used S1 or S2 or S3 as strings for full-text search, resulted in more than 92,000 hits. After filter the C1 strings, the result remained more than 50,000 hits. In order to assure the accuracy of the result, we change S1 or S2 or S3 not C1 as strings for abstract search (change the pefix to AB). After applying the different in-/exclusion criteria and peer review procedures, 109 papers were selected for further analyse.

Table 5. Overviews of the results obtained from the literature search.

Step \ Databases	CJFD	CDFD	CMFD	Total
Step1: Search (S1 or S2 or S3)	14956	10630	66873	92459
Step2: Filtering				
Not C1	12176	7387	33412	52975
Change FT (full text) to AB (abstract)	45	72	446	563
Final result set (after peer review)	28	36	45	**109**

According to the publication frequency over time (1984-2016), we classified the sources to illustrate the development of the considered domain over time, as Figure 2.

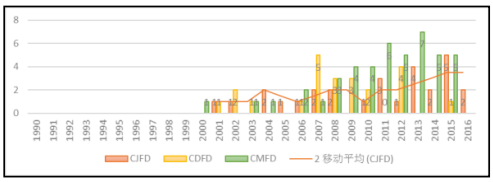

Fig. 2. Numbers of papers per year and distribution over the sources.

From Figure 2, we see the field of safe-critical software development of industrial robots which has been paid close attention since 2000, being a still emerging trend in China. Since then, we observed the majority of the published papers. From the data sources, we can see that there still have a big gap between the evaluation researches and the engineering practices, as three quarters of papers are written by graduate and doctoral students.

3.4.2 RQ1: what standards or certifications for industrial robot software development have been adopted in domestic?

Functionally safe systems are developed and validated against well-defined market-specific functional safety criteria. The umbrella standard for the majority of application-specific functional safety development in electronics is IEC 61508. It specifically addresses electrical, electronic and programmable electronic safety-related systems. Many market specific safety standards and guidelines have been derived from IEC61508. To present the standards or certifications for industrial robot software development in domestic, a systematic analysis is provided as Table6.

Table 6 illustrates the research- and standards type facets and shows the majority of the papers which still do not follow the safety standards in software development of industrial robots (68 out of 109). Table6 also illustrates that there are more pre-researches in colleges (81 out of 109). That is, the current publication body is focused on proposing fundamental researches to deal with the challenges coming along with developing safety-critical software for industrial robots. Nonetheless, table6 points to an emerging field.

3.4.3 RQ2: What practices are used for the development of safety-critical software for industrial robotic systems (including coding and testing)?

Integrating software onto a specific processor and hardware environment is one of the most challenging areas of a system to develop and assess demanding certification requirements. Table 7 shows that many different aspects are covered and that many different practices are addressed, especially verification of the software architecture design and software testing. However, 60 papers are classified into the others, meaning that there has not safety-related software development practices. Therefore, table7 indicates that, the safety-critical software development of industrial robots in domestic are not according to the prescribed standards or certifications. Nevertheless, there are some practices such as software simulation and software testing, which are implemented widely in software development of industrial robots.

3.4.4 RQ3: Which certification standards have provided feasible implementation guidelines for software for industrial robots?

This question aims at investigating whether current certification standards have provided feasible implementation guidelines for the software of industrial robots. Therefore, we collected the major standards addressing this topic for

general safety-critical software development (Table4). According to 4.4.2, we found that a loose connection between software development practices and available standards. Only the IEC 61508 (general functional safety standard) was mentioned by those papers. However, the standard ISO 10218 (Robots and robotic devices—Safety requirements for industrial robots) was not referred at all! Thus, although software safety is becoming more critical due to the increasing number of industrial systems controlled by software, there are no feasible implementation guidelines of these standards to achieve safety requirement.

Table 6. Systematic analysis illustrating papers vs standards.

	ISO 10218	IEC 61508	IEC 61131-6-2012	IEC 61511-2003	IEC 61499	Guaranteeing safety	Non-Standard Approach
CJFD	0	4	1	0	0	9	14
CDFD	0	4	2	2	0	4	24
CMFD	0	7	1	0	0	7	30
Total	0	15	4	2	0	20	68

Table 7. Systematic analysis illustrating papers vs software development practices.

	Notations for architectural design	Error detection at the software architectural level	Error handling at the software architectural level	Verification of the software architectural design	Notations for software unit design	Verification of software unit design and implementation	Methods for software testing	Methods for deriving test cases for software testing	Others
CJFD	2	3	1	6	2	2	4	1	16
CDFD	3	3	5	7	4	4	5	2	16
CMFD	2	1	5	3	3	1	7	1	28
Total	7	7	11	17	11	9	16	3	60

4 Conclusion

Over recent years, there has been a drastic increase in the numbers of software usage in safety-related systems. Several safety-related systems such as industrial robot systems depend on software to manage the safety-related functionalities. The last several years have seen a sharp resurgence in the orders of industrial robots in China, and the areas addressed within industrial robotics has extended into safety-critical domains. The demand for software in industrial robots is expected to increase in the following years which turn out to be a challenge in the software safety and requirement engineering processes. This paper presents a systematic analysis of functional safety certification practices in software development for the safety-critical software of industrial robots, to identify the safety certification practices used for the development of industrial robots in China and how these practices comply with the safety standard requirements. Our research from reviewing Chinese academic papers, shows that safety standards are barely used in software development of industrial robot. The majority of the papers propose various solutions to achieve safety, but only about two thirds of the papers refer to non-standardized approaches that mainly address the systematic level rather than the software development level. In addition, our research shows that as the development of artificial intelligent, an emerging field is still on the quest for standardized and suitable approaches to develop safety-critical software.

The present study is a first step toward a deeper understanding of safety certification in industrial robot development. In future, we need to do further research on safety-related standards of industrial robots such as (IEC 61508, ISO 10128 etc.), to establish a feasible implementation guideline for software for industrial robots. Our end objective is not to meet safety standards or to pass the assessment test, but to actually deliver an industrial robot system that is functionally safe.

References

1. International Standard 8373:2012: Robots and Robotic Devices - Vocabulary. International Organization for Standardization (2014)
2. MISRA: MISRA-C Guidelines for the Use of the C Language in Critical Systems (2012)
3. International Standard ISO 25119-2010: Tractors and machinery for agriculture and forestry - safety-related parts of control systems, International Organization for Standardization (2010)
4. International Standard ISO 26262:2011: Road Vehicles Functional Safety, International Organization for Standardization (2011)
5. Dogramadzi, S., Giannaccini, M.E., Harper, C., Sobhani, M., Woodman, R., Choung, J.: Environmental hazard analysis - a variant of preliminary hazard analysis for autonomous mobile robots. J. Intell. Rob. Syst.**76**(1), 73–117 (2014)
6. International Standard ISO 13482:2014-Robots and robotic devices - Safety requirements for personal care robots. International Organization for Standardization (2014)
7. Jacobs, T., Virk, G.S.: ISO 13482 - the new safety standard for personal care robots. International Symposium on Robotics (ROBOTIK 2014), pp. 1–6. VDE-Verl (2014)
8. International Standard ISO 10218:2011- Robots and robotic devices—Safety requirements for industrial robots. International Organization for Standardization (2011)
9. Cochrane Handbook for Systematic Reviews of Interventions [EB/OL] / [2009-7]. http://www.cochrane-handbook.org/
10. Australian National Health and Medical Research Council. *How to Review the Evidence: Systematic Identification and Review of the Scientific Literature: Handbook Series on Preparing Clinical Practice Guidelines* (2000)
11. NHS Centre for Reviews and Dissemination Undertaking Systematic Reviews of Research on Effectiveness. CRD Guidelines for Those Carrying Out or Commissioning Reviews. University of York, York. (1996)
12. B.Kitchenham. Procedures for Performing Systematic Reviews. Keele University Technical Report TR/SE-0401 (1999)
13. K.Petersen , R.Feldt, S.Mujtaba, M.Mattsson: Systematic mapping studies in software engineering. In: International Conference on Evaluation and Assessment in Software Engineering, pp. 68–77. British Computer Society (2008)