10

Experiences Developing Safe and Fault-Tolerant Tele-Operated Service Robots. A Case Study in Shipyards

Diego Alonso, Pedro Sánchez, Francisco J. Ortiz, Juan A. Pastor,
Bárbara Álvarez and Andrés Iborra
Division of Electronics Engineering & Systems (DSIE)
Universidad Politécnica de Cartagena
Spain

1. Introduction

Human operators use tele-operated service robots for performing more or less hazardous operations (manipulation of heavy and/or dangerous products) in more or less hostile environments (nuclear reactors, space missions, warehouses, etc). Anyway, independently of the operation, the robot has to interact with both the environment it is working on and with human operators. Therefore, it is essential that the design (which include both software and hardware) of the robot involves no risk, or at least an acceptable level of risk, neither for the operators, nor for the environment nor for the robot itself.

Nevertheless, it is not always possible to make a system free of failures in its design or operation. Apart from the risk inherent to the use of the mechanisms themselves, these systems work in hazardous environments, where the probability of the risk is higher than normal. Should a failure happen, its consequences could even involve the loss of human lives. (Neumann, 1994) documents many cases of computer-related failures, such as the Therac-25 (a radiation-therapy device), the missiles shield in Saudi Arabia, etc.

Nevertheless, safety aspects are seldom included in the early phases of the system design process from the beginning, even though they are a critic aspect. Generally, safety has to conform and adapt to the already designed system and not vice versa, when it is widely known that safety involves not only the design of the software but also the hardware. Even more, a simple hardware solution can eliminate a hazard or simplify the software design in many situations.

However, the identification of safety requirements should not be different from the identification of the rest of requirements of the system. It only requires a more thorough study due to their importance (human lives and equipment integrity may depend on it). On the other hand, safety has a big repercussion in both the specification and design phases, especially when the time to define the architecture of the system arrives. Its impact is even bigger by the need to avoid common failure modes, which can propagate failures within different units of the system.

There are a number of standards and techniques for addressing safety requirements in electronic devices in general and for industrial arm robots, but none specifically designed

for addressing the elicitation of safety requirements or for proposing software/hardware solutions in the domain of service robots.

With more than twelve years of experience in the design of software applications for tele-operated service robots (Iborra et al., 2003; Fernández et al, 2005), the DSIE research group at the Universidad Politécnica de Cartagena has developed several tele-operated service robots in the context of the **EFTCoR**[1] project (*Environmental Friendly and Cost-Effective Technology for Coating Removal*). This project was part of the European Industry effort to introduce environmental friendly ship maintenance. The EFTCoR project addressed the development of a solution to the problem of retrieval and confinement of the sub-products obtained from the ship maintenance operation (oxide, paint and adherences mainly). The variability of the domain (hull dimensions and shapes differ widely) and hard working conditions for robotic devices, imposed the design of different robotic systems, each adapted to the specific problem. In such a dangerous and hazardous environment, it is compulsory to address, from the beginning of the project, both the hardware and software safety requirements in order to design safe robots.

The main objectives of this chapter are (1) to stress the importance of capturing the safety requirements early in the design process, and (2) to present a systematic approach, based in both standards and some traditional safety techniques and solutions, that could guide other designers considering safety requirements from the beginning of their projects.

In order to illustrate such a systematic approach, we expose a thorough study of the safety requirements that a crane robot (a member of the EFTCoR project) had to conform to in order to work in such a hazardous environment as shipyards are. The design decisions adopted to conform such safety requirements will be also presented.

This chapter is structured in five sections. Section two details the state of the art in safety standards and techniques. The following two sections are devoted to the description of the safety requirements elicitation methodology and an example of its application in the context of the design and development of the EFTCoR crane robot. Finally, section five summarises the main results and conclusions extracted from our experiences and outlines future lines of work. The complete tables of the proposed elicitation process are presented in the appendix, at the end of this book chapter.

2. Survey of safety standards and techniques

Before going on, we introduce the meaning of some of the terms that appear in this chapter. According to (Douglass, 2003), a *risk* is an event or condition that can occur but is undesirable; *safety* is the characteristic of a system that does not incur too much risk to persons or equipment and an *accident* is damage to property o harm to persons, the happening of a risk. A *safety system* is, according to the definition of ANSI/RIA (Ansi/Ria, 1999), a system that has been tested, evaluated and proven to operate in a reliable and acceptable manner when applied in a function critical to health and welfare of personnel. According to (Leveson, 1995), a *hazard* is a state or set of conditions of a system (or object)

[1] The EFTCoR (http://www.eftcor.com) project was founded by the EU 5th Framework Programme (GROWTH G3RD-CT-00794) with 2M€. It included ten partners from six European countries.

that, together with other conditions in the environment of the system (or object) will inevitably lead to an accident (loss event).

There are several approaches to manage safety in the literature, but they are either too general or not specifically targeted at the tele-operated robot domain. Many deal with the problem of designing a standard that guides the whole process (from identification to solution) while others are simple tools or techniques. Among these standards, we want to stress the European Standard EN 61508:2001 (EN 61508, 2003) and the American ANSI/RIA R15.06-1999 (Ansi/Ria, 1999). Among the techniques for safety designs it is worth highlighting fault trees analysis (Hansen et al., 1998) and **ROPES** (Douglass, 1999) (*Rapid Object-oriented Process for Embedded Systems*).

- **EN 61508:2001**. This European standard sets up a generic approximation for dealing with all the activities related to the life cycle of the systems that use electric and/or electronic and/or programmable devices for safety functions. The other main purpose of this standard is to serve as a basis for the development of specific standards for each application sector, which would take into account techniques and solutions typical of the sector.
- **ANSI/RIA R15.06-1999**. The objective of this standard is to enhance the safety of personnel using industrial robot systems by establishing requirements for the manufacture (including remanufacture and overhaul), installation, safeguarding methods, maintenance and repair of manipulating industrial robots. It is the intention of this standard that the manufacturer (including re-manufacturer and re-builder), the installer and the end-user have specific responsibilities.
- **Fault trees**. It is one of the most popular approaches to identify, evaluate and manage safety requirements. These trees provide a graphical notation and a formal support that makes it easy to make the analysis from the perspective of the system failures and their origins. However, they do not offer a global framework for requirement specification as a discipline.

ROPES is, in words of Douglass, "*a development process that emphasises rapid turnaround, early proofs of correctness and low risk*". ROPES is an iterative process that organises the design process in small, incremental steps. Douglass proposes an eight-step methodology for dealing with the safety aspects of any system.

3. Description of the safety requirements elicitation process

As already outlined, there is no specific standard or methodology for addressing the elicitation of safety requirements for service robots, or for proposing software/hardware solutions that fulfil them. Instead, there are a number of standards and techniques for addressing safety requirements in electronic devices in general, and for industrial arm robots, but none specifically designed for service robots.

In this vein, this work presents a systematic approach, based in both standards and some traditional safety techniques and solutions, which could guide other designers considering safety requirements from the beginning of their projects.

As last section shown, until a new standard derived from EN 61508 and targeted at robotics appear, only the ANSI standard offers a specific guide that is close enough to the domain of tele-operated robots so that it can be adapted to this domain.

In order to complete those aspects not covered by the standard ANSI, the proposal "*eight steps to safety*" from Douglass (Douglass, 1999) has been adopted and adapted. In this work, Douglass proposes some design patterns oriented to the achievement of a particular safety objective, such as *multi channel voting pattern, watchdog pattern, safety executive pattern*, etc. By using these patterns, it is possible to design software solutions that conform to the needs imposed by the ANSI standard, according to the level of risk of a particular hazard.
Finally, *fault trees* could be used to obtain the possible causes of the failures that are analysed in second step of the methodology we propose. Fault trees analysis is a very used and mature technique, but it does not help measuring, classifying or solving failures, and thus, we have not applied this technique.
The four-step methodology presented in this chapter proposes the fusion of the standards and techniques presented in the previous section. It encourages the tracking of safety throughout the life cycle of the robot (as EN 61508 proposes) and uses the ANSI standard as a guide to classify hazards and to propose solutions. By completing ANSI with the contributions of ROPES, it is possible to deal with the design of software-based solutions that are more complex than a simple barrier. Figure 1 depicts a diagram showing the different steps that make the proposed methodology up.

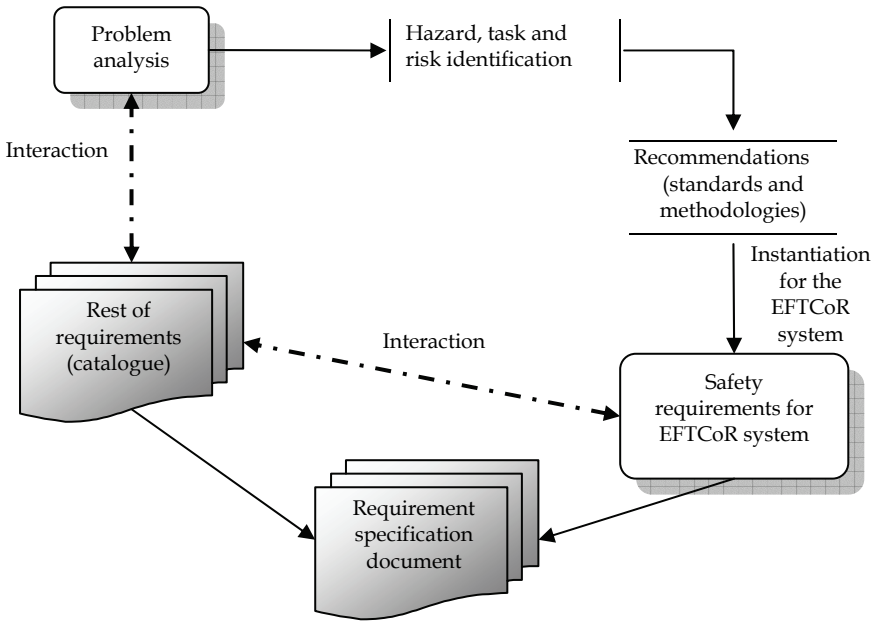


Fig. 1. Safety-driven requirements elicitation methodology.

STEP 1 ► Identify hazards
It is desirable that a system should normally work without imminent hazards. Therefore, the first step is to identify all the tasks that involve the use of the system and that have potential hazards. After that, each task is analysed for describing the hazards associated to it. Some

possible sources for the identification of hazards, which can serve as a starting point in their identification, are the following ones (extracted from (Ansi/Ria, 1999)):

- The movement of mechanical components, especially those that can cause trapping or crushing.
- Stored energy in moving parts, electrical or fluid components.
- Power sources: electrical, hydraulic, pneumatic, etc.
- Hazardous atmospheres, material or conditions: explosive or combustible, radioactive, high temperature and/or pressure, etc.
- Acoustic noise, vibrations, EMI, etc.
- Human failures in design, construction, installation, and operation, whether deliberate or not.

This analysis of hazards also include the identification of the possible causes of the failure (hardware, software or human), the task in which it can happen, the reaction to the happening of the hazard, and some temporal data (adopted from ROPES (Douglass, 2002)). These time related parameters try to quantify (1) how long the hazard can be tolerated before it results in an accident (*tolerance time*), (2) the maximum amount of time to detect the happening (*detection time*), and (3) the maximum time to react to it (*reaction time*).

STEP 2 ► Identify risks

The objective of this second step is to (1) identify the possible risks of the system, (2) classify them according to the impact they have on the environment, and (3) link them to the hazards identified on the first step. The ANSI standard states that three characteristics have to be evaluated for each identified risk: its level of severity, its level of exposure and its level of avoidance. Each of these characteristics has two different values, resulting in eight possible combinations. Depending on the different values of these characteristics, a **RRC** *(Risk Reduction Category)* is obtained (see Table 1). Based on the RRC, ANSI requires a certain level of performance of the safeguard and circuits that are to be design to reduce the risk (simple, single channel, single channel with monitoring and control reliable). Moreover, ANSI also recommends the adoption of safety policies to help human operators avoid some risks (training, presence detectors, security barriers, etc).

After applying the safeguards designed for the specific RRC, a new analysis is performed to calculate the residual risk, just to be sure that the risk is kept at a tolerable level for both the system and the environment. This process does not end here, but has to be repeated during the life cycle of the robot to ensure that no new risk appears and that the risks already identified are kept under control.

STEP 3 ► Specify safety requirements

The purpose of this third step is to extract the system safety requirements from the results of the previous steps. This step is quite difficult to perform because neither the ANSI standard nor ROPES offer a methodology to deduce the requirements from the previous results, so this extraction has to be manually done. For addressing this third step, it is necessary to have or develop:

1. An appropriate process for requirement harvesting.
2. A way to catalogue them, in order for the requirements to be reused in other systems of the domain of application (tele-operated robots in this case).
3. Tools for tracing the use of the requirements throughout the development process and, in particular, until designing the architecture of the system.

RRC	Procedure	Control level
R4	Safeguarding, at a minimum, shall be by administrative means, awareness means including audio/visual warnings and training.	Simple Control (consult next table).
R3A, R3B	Non-interlocked barriers, clearance procedures and equipment.	Choose between Single channel and Simple Control (consult next table).
R1	Hazard elimination or hazard substitution	Control Reliable (consult next table).
R2A, R2B, R2C	Preventing access to the hazard or stopping the hazard (interlocked barrier guards, etc.)	Choose between Control Reliable, Single Channel or Single Channel with Monitoring (consult next table).

Description of the different control levels
1. Control reliable safety circuitry shall be designed, constructed and applied such that any single component failure shall not prevent the stopping action of the robot. These circuits shall be hardware based, and include automatic monitoring at the system level: a) The monitoring shall generate a stop signal if a fault is detected. A warning shall be provided if a hazard remains after cessation of motion; b) Following detection of a fault, a safe state shall be maintained until the fault is cleared. c) Common mode failures shall be taken into account when the probability of such a failure occurring is significant. d) The single fault should be detected at time of failure. If not practicable, the failure shall be detected at the next demand upon the safety function. 2. Single channel safety circuits shall be hardware based or safety related software and firmware based controllers, include components which should be safety rated, be used in compliance with manufacturers' recommendations and proven circuit designs. 3. Single Channel with Monitoring safety circuits shall include the requirements for single channel, shall be safety rated, and shall be checked (preferably automatically) at suitable intervals. a) The check of the safety function(s) shall be performed at machine start-up, and periodically during operation; b) The check shall either: allow operation if no faults have been detected, or generate a stop signal if a fault is detected. A warning shall be provided if a hazard remains after cessation of motion; c) The check itself shall not cause a hazardous situation; d) Following detection of a fault, a safe state shall be maintained until the fault is cleared. 4. Simple Control. Simple safety circuits shall be designed and constructed using accepted single channel circuitry, and may be programmable.

Table 1. Risk Reduction Category explanatory table (extracted and summarised from ANSI).

STEP 4 ► Make safe designs
The design of the software architecture of the system must consider the safety measures and avoid failures that spread through the whole system. A safe design must start with the previous security requirements (third step) to adopt a concrete architectural pattern that could be periodically reviewed when new hazards are identified. To be able to do it, to be able to be adaptable, a rigorous architectural approach that allows the evolution of the architectural model due to new requirements or by evolution of the conditions of work is necessary (which is also out of the scope of this book chapter).

4. Application of the elicitation process in the context of the EFTCoR project

This section describes the application of the safety requirements elicitation methodology in the context of the EFTCoR project in order to come up with a design that satisfies the safety requirements of the robot. The early analysis of the possible hazards and safety conditions allowed us to make the hardware and software design of the robot addressing the safety requirements from the beginning. Specifically, this section is divided into the following sub-sections:

- Section 4.1 briefly describes the objective of the EFTCoR project, the working environment, and the solution developed by the DSIE research group.
- Section 4.2 presents the EFTCoR commercial crane and the application of the proposed safety requirements elicitation methodology to refine its design. The exhaustive compilation and classification of the safety requirements presented in this sub-section can be consulted in the appendix.

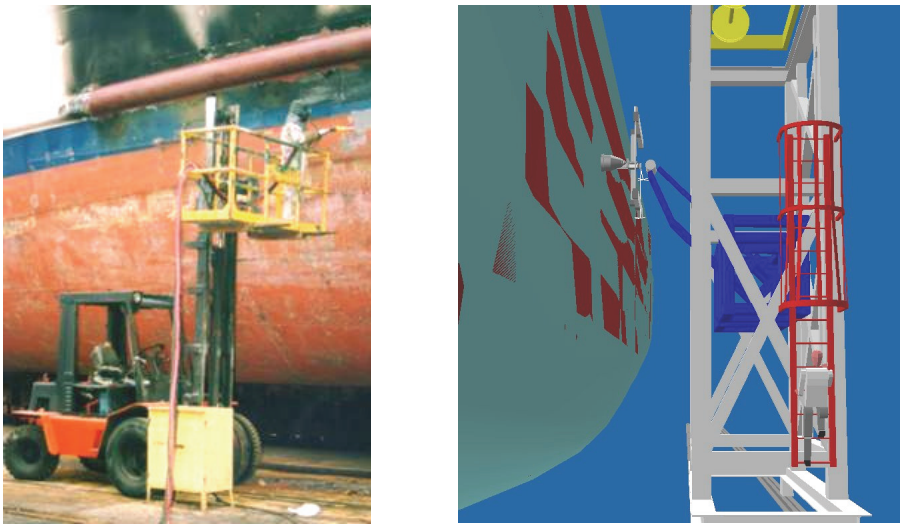
4.1 Brief overview of the EFTCoR project

The EFTCoR family of robots offers a global environmentally friendly solution to the problems related to the most dangerous hull maintenance operations. These operations consist of periodic (every four to five years) removal of sea adherences and the hull coating followed by hull repainting. These operations preserve the hull integrity, guarantee safe mailing conditions, and maintain a smooth hull surface, which minimizes fuel consumption, reduces operating costs, and prevents excessive atmospheric contamination. Other maintenance operations are scheduled or even delayed to coincide with hull cleaning and repainting. The existing hull cleaning technology, grit blasting (see Figure 2-a) (IMO, 1999), is highly pollutant, environmentally unaffordable, dangerous for human operators, and it is progressively being banned in Europe. The solution developed in the context of the EFTCoR project comprises two families of robots:

- Tele-operated cranes with blasting tools for cleaning big areas (what is called "*full blasting*"), normally a ship vertical surface.
- Tele-operated climbing vehicles with a small blasting tool for cleaning small areas (what is called "*spotting*"), normally a ship bottom or bow.

All these robots consist of a primary positioning system, capable of covering large hull areas, and a secondary positioning system, mounted on the primary system, that can position a tool over a relatively small area (from 1 to 16 m^2). These robots have been developed to achieve the objective of performing the current hull cleaning operations in a way that avoids the emissions of residues to the environment and enhances the working

conditions of the shipyard operators without worsening the current costs and operation times (see Figure 2-b).



a) Before EFTCoR b) With EFTCoR crane

Fig. 2. Manual vs. automatic blasting operation.

The design of such a complex system as the EFTCoR involves the necessity of early detection and identification of failures so that correcting measures can be adopted early in the design of the robot. The fundamental characteristics of the EFTCoR that makes it compulsory to take into account the need of a safe approach when designing the robots are summarised by the following points:

- The operator uses a heavy mechatronic device whose range of movement can cause serious damage (see Figure 2-b).
- Some maintenance operations include the blasting of the hull with high-pressure abrasive particles. The energy of the jet makes it very dangerous for human operators and for the rest of the equipment, so it is necessary to train operators in the use of the tool, to maintain the equipment in perfect conditions and to install all the security components needed. In addition, the impact of the jet over the ship hull produces a lot of dust, worsening the condition of the working place.
- The system has to be designed for working outdoors, so it has to be able to deal with atmospheric agents that can alter its normal operation (rain, water on the ground, dust, noise, wind, etc.).
- The working environment of the robots (shipyards) is very dynamic: there are many cranes, load and unload of heavy equipments, many operators moving around (either working on the robot or conscious or not of its presence), etc.

4.2 Application of the proposed safety requirements elicitation methodology

This section describes in detail the application of the proposed methodology to the design of the EFTCoR crane robot. This robot is composed of a commercial crane as the primary

positioning system and a cartesian robot (XYZ table) as the secondary positioning system (see Figure 3). The crane has its own control (provided by the manufacturer), a height of twelve meters and a weight of twenty tons, which make unavoidable the movement of the robot with the consideration of safety requirements. It also has, in its central zone, an articulated arm of two tons for holding the XYZ table (which includes a cleaning tool). The control system of the XYZ table has been designed to follow the cleaning instructions from a human operator or from a computer vision system, which locates the areas of the hull that have to be blasted and commands the crane robot.

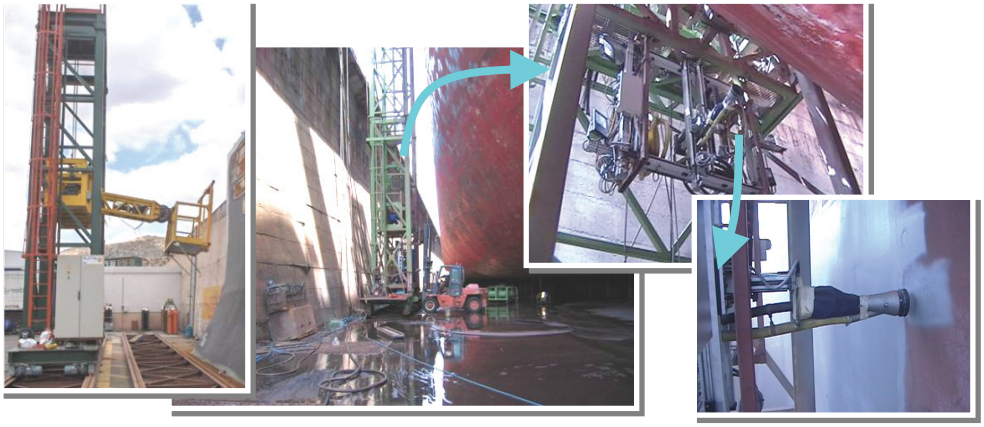


Fig. 3. Crane robot for cleaning vertical surfaces in EFTCoR.

STEP 1 ► Identify hazards

Starting from the functional requirements of the EFTCoR system (which were part of the initial project proposal), thirty different tasks with a potential hazard were identified (see Table 2). As shown in the table, these tasks are performed not only by the operator of the robot but also by the maintenance and cleaning staff, they can have been planned or not, and their frequency can be daily, weekly, monthly, annually, etc.

Afterwards, the hazards related to the tasks to be performed by the robot (which are shown in Table 2) have to be identified. Table 3 shows (an excerpt of) the thirty one identified hazards and classifies them according to the tasks in which they can appear, the risk level associated to the hazard, the possible sources for the hazard, and their probability, as all these characteristics are needed to perform the following step. Table 3 also outlines some of the reaction measures that can be adopted to minimise the effects of the corresponding hazard. The *first step* of the proposed methodology ("identify hazards") is fulfilled after the elaboration of these two tables. Lastly, it is worth highlighting that:

- There is no direct relationship between the number of tasks a system must perform and the number of hazards that can be identified and characterised.
- There is no methodology that can help finding the corresponding hazards and their possible sources. This process depends on the domain and the requirements of the system, although a mature technique such as fault tree analysis could help finding them.

Task	Type	Description
T1	operator	Move the primary positioning system (rail)
T2	operator	Move the primary positioning system (vertical axis)
T3	operator	Move the primary positioning system (arm)
T4	operator	Coordinate the primary positioning systems for positioning the secondary positioning system (XZY table)
T5	operator	Move one of the axis of the secondary positioning system (XYZ table)
T6	operator	Coordinate the secondary positioning system axes (XYZ table)
T7	operator	Execute a sequence of movements of the secondary positioning system.
T8	operator	Execute a sequence of movements of the primary positioning system.
T9	operator	Activate the cleaning tool
T10	operator	Deactivate the cleaning tool
T11	operator	Execute an emergency stop of both positioning systems
T12	operator	Stop the primary positioning system (rail)
T13	operator	Stop the primary positioning system (arm and vertical axis)
T14	operator	Stop the primary positioning system (XYZ table)
T15	operator	Disable axis
T16	operator	Change movement/control parameters
T17	operator	Change working mode (manual/automatic)
T18	operator	Restock grit.
T19	operator	Test robot anchors
T20	maintenance	Calibrate primary positioning system
T21	maintenance	Calibrate secondary positioning system
T22	maintenance	Calibrate machine vision system
T23	maintenance	Repair one of the axis (primary or secondary positioning system)
T24	maintenance	Manually tool assembly
T25	maintenance	Manually tool disassembly
T26	maintenance	Substitute video wire
T27	maintenance	Substitute/repair the grit-blasting tool.
T28	maintenance	Substitute/repair the communication infrastructure
T29	maintenance	Substitute/repair the control infrastructure
T30	cleaning	Clean the machine vision system

Table 2. Task list of operations that can be performed when using the robot.

STEP 2 ► Identify risks

The *second step* starts from the results previously obtained in Table 3. In this step, different risks are evaluated and described for each hazard (see excerpt in Table 4). Each risk is characterised from different points of view (severity, exposure and avoidance, shown in the complete table in the appendix) and then associated a given RRC (consult Table 1), according to these characteristics.

Hazard	Task	Risk Level	Origins	Prob.	Reaction measures
H1. The cleaning tool hits the ship hull	T5-7, T21	Severe	Breakage or error in the axis controller. Comm. failure (logic or physic)	Low	Emergency alarm[2] Stop axis and move it away from the hull. Power axis off.
H2. Over exposure of the tool or delayed deactivation.	T10	Slight	Breakage of an axis of the secondary positioning system or the tool. Software scheduling error. Communication failure.	Low	Emergency alarm. Power tool off. Stop grit-blasting.
H3. Workers in the trajectory of the primary positioning system (rail).	T1	Very severe	There is a person in the trajectory of the movement of the primary positioning system.	Med.	Emergency alarm. Stop the robot. Emergency stop.
H4. Equipment in the trajectory of the primary positioning system (rail).	T1, T20	Severe	There is an obstacle in the trajectory of the primary positioning system.	Med.	Emergency alarm. Stop the robot. Emergency stop.
H5. Obstacle in the trajectory of the primary (vertical axis or arm).	T2-4, T20	Very severe	There is an obstacle in the trajectory of the primary positioning system.	High	Emergency alarm. Stop the robot. Emergency stop.
H6. Obstacle in the trajectory of the secondary positioning system.	T5-8, T21	Very severe	There is an obstacle in the trajectory of the secondary positioning system.	Low	Emergency alarm. Stop the robot. Emergency stop.

Table 3. Excerpt of the hazard identification list. Consult complete table in the appendix.

Afterwards, a series of solutions to leverage the risk are proposed, and the hazard is re-evaluated (severity, exposure and avoidance levels) to verify its new RRC. Depending on the final RRC value, additional measurements should be taken into account to leverage the remaining risk, re-evaluating the system again, until the needed residual RRC is finally achieved. For instance, the hazard H1 in Table 4 (consult appendix) was evaluated to have a severity level S1, an exposure level E2 and an avoidance level A1. According to the ANSI standard, these levels result in an RRC level R3A.

[2] Different alarm levels: visual, acoustic, etc, depending on the severity.

STEPS 3 and 4 ► Specify safety requirements and Make safe designs
The application of the steps 3 and 4 of the proposed methodology is out of the scope of this book chapter. Specifically, in step 3 a catalogue of safety requirements for the family of robots is extracted with the purpose of being able to reuse it when developing similar robots. We are currently developing a CASE tool for easing the reutilization of this catalogue.

Hazard	Risk	RRC	Solution	RRC
H1. The tool hits the ship hull.	R1. Tool breakage or damage to the secondary positioning system.	R3A	Add bumpers to the head of the tool. Limit Z-axis maximum torque.	R4
H2. Overexposure of the tool or delay in its deactivation.	R2. Damage to the ship hull surface.	R3A	Add a software timer (compliant with 6.4 ANSI) to control the tool working time. Add a motion sensor to the secondary positioning system and link it to the timer.	R4
H3. Workers in the trajectory of the primary positioning system (rail).	R3. Worker run over.	R2A	Add sensors to detect obstacle presence in the rail. These sensors are directly wired to the robot safety control infrastructure. Add a siren for signalling robot motion.	R3B
H4. Equipment in the trajectory of the primary positioning system (rail).	R4. Damage to the equipment and to the primary positioning system.	R2A	Same as H3	R3B
H5. Obstacle in the trajectory of the primary (vertical axis or arm).	R5. Damage to the primary and to the obstacle	R1	Add sensors for detecting obstacles in the trajectory of the arm and wire them to the robot safety control infrastructure.	R3B
H6. Obstacle in the trajectory of the secondary positioning system.	R6. Damage to the secondary or to the tool	R2B	Hw/Sw torque control for detecting overload.	R4

Table 4. Excerpt of the hazard identification list. Consult complete table in the annex.

Regarding step 4, the impact of considering the previously obtained safety solutions on the software architecture of the robot is detailed in Table 5, while the impact on the robot hardware design has already been summarised in Table 4.

4.3 Brief summary of the application of the methodology

This last sub section presents a brief summary of the conclusions that can be extracted from the whole study presented in this book chapter. To do so, the thirty one identified hazards (shown in Table 3 in the appendix) have been classified in six groups, depending on the type of safeguard adopted (consult Table 5). The percentage shown in the last column of Table 5 is relative to the total number of safety requirements that were present in the EFTCoR project initial proposal, sixty in total.

The following conclusions can be extracted from this study:

- **Forty five percent** of the safety requirements do not affect the architectural design neither its possible evolution.
- **Fifty five percent** of the safety requirements do affect software architecture, of which:
  - **Forty percent** imply the addition or extension of some components so that the state of the actuators can be double-checked.
  - **Six dot six percent** imply the design and adoption of redundant nodes.
  - **Eight dot six percent** imply the addition of new sensors to the robot to monitor the system (generally, safety-related sensors).

	Solution kind	Related hazard	Total safety req
Solution affects Sw architecture	Addition of safety Sw modules in the robot control unit.	H2, H14, H16, H17, H21	**8.33%**
	Addition of extra safety elements controlled by Sw modules (e.g. emergency stop, alarm bells and lights, etc).	H1, H2, H3, H3, H4, H4, H5, H10, H12, H12, H13, H13, H15, H15, H21, H22, H25, H25, H24, H26, H26, H28, H31, H27	**40%**
	Addition of redundant Sw safety modules and systems.	H10, H23, H5, H11	**6.66%**
			subtotal 55%
Solution does not affect Sw architecture	Addition of electrical/mechanical limiting elements.	H1, H6, H7, H8, H9, H18, H18, H19	**13.33%**
	Specification of usage and signalling procedures (e.g. cleaning, adding beacons, etc.).	H10, H24, H24, H28, H31, H25, H26, H27, H28, H28	**16.66%**
	Use of safety certified elements (e.g. connectors, wires, etc.).	H20, H20, H21, H21, H26, H29, H30, H30, H31	**15%**
			subtotal 45%

Table 5. Conclusions of the application of the methodology.

5. Conclusions and future research

When a system interacts with the environment and/or with humans, the analysis of possible hazards that could occur during its operation becomes indispensable. Nevertheless, this analysis is a complex process that needs the support of a methodology. The more domain-specific the methodology, the more accurate the results will be.

In the context of the EFTCoR project, the DSIE has developed a series of robots for ship hull cleaning in such a hazardous environment as shipyards are. In order to fulfil the safety requirements of the EFTCoR project, we have adopted a systematic approach for addressing them from the beginning of the design phase. In this book chapter, we have described a complete example of the application of the process to a real service robot that works in an aggressive industrial environment. This example considers not only the safety requirements elicitation process but also the classification of the different hazards and the proposed solutions to them.

The proposed safety requirements elicitation process is based on a mix of different techniques and standards, as no single standard or technique address all the different, hardware and software, aspects involved in the development of a service robot.

We have used the ANSI/RIA standard as the basis for the identification and classification of the hazards, risks and the safeguards to be adopted to reduce the risks to acceptable levels. This standard has being completed with the safety patterns extracted from Douglass when designing a more complex solution and the use of fault trees to identify the possible causes of failure. In this sense, we hope that a European standard, derived from EN 61508 and specifically targeted to robotics systems, will soon appear to fulfil the lack of a methodology for safety requirements specification and solutions in the EU.

Although it may seem that this work is the result of applying together ("glued" even) several standards, the contribution of this work goes further on because:

- It gathers the methodological experience of diverse authors, since this experience is usually absent in most of the standards.
- The range of application of the proposal is wider than that of one of a single standard or technique seen in section 3, because this work covers from requirements specification to the implementation patterns applied in architectural design.
- Lastly, a case study of a real application has been presented, where the safety requirements were naturally present from the beginning of the project, not added later.

Two important conclusions can be extracted from this work: (1) only half of the safety requirements really affect the software architecture of the system, and (2) only a few fractions of them require the use of external redundant control that must conform to the strictest level of safety. Nevertheless, since security requirements are, conceptually, independent of the functional ones, it would be more than desirable to have an architectural approach that allows designers to consider them in isolation.

We are currently working on the adoption of a *Model-Driven Engineering* (Stahl & Völter, 2006) approach to develop the software architecture of a robot starting from a model. In this vein, we plan to:

- Adapt and include the proposed safety requirements elicitation process as an orthogonal aspect, in order to map the solutions to these requirements to the software architecture of the robot.

- Develop a safety requirement catalogue and some heuristics to help designers take into account safety requirements from the beginning of the design.
- Keep a traceability record of the implementation of the safety solutions in the software architecture (and later in the generated code) of the robot.

Lastly, we want to conclude this book chapter stating that it contributes not only the experience of the DSIE research group in the application of different standards and methodologies, but also a complete example in the context of a real problem. We hope that the tables presented in the appendix could help designers and engineers as a starting point when developing similar systems. To our knowledge, there is no such a complete example in the literature as the one we have described in this book chapter.

6. Acknowledgements

This research has been funded by the Spanish CICYT project MEDWSA (TIN2006-15175-C05-02) and the Regional Government of Murcia Seneca Program (02998-PI-05).

7. References

ANSI/RIA R15.06 (1999), American National Standard for industrial robots and robot systems safety requirements. Robotic Industries Association.

Douglass, B. (1999), Doing hard time: developing real-time systems with UML, objects, frameworks and patterns. Addison-Wesley Longman. ISBN: 0-201-49837-5.

Douglass, B. (2002), Real-Time Design Patterns: Robust Scalable Architecture for Real-Time Systems. Addison-Wesley Professional. ISBN 0201699567.

EN 61508 (2003), Functional safety of electrical/electronic/programmable electronic safety-related systems. European Committee for Electro-technical Standardization.

Fernández, C.; Iborra, A.; Álvarez, B.; Pastor, J.; Sánchez, P.; Fernández, J. & Ortega, N. (2005). Ship shape in Europe: cooperative robots in the ship repair industry, IEEE Journal on Robotics and Automation, vol. 12, num. 3, pp. 65-77. ISSN 1070-9932.

Hansen, K.; Ravn, A. & Stavridou, V. (1998). From safety analysis to software requirements. IEEE Transactions on Software Engineering, vol. 24, num. 7, pp 573–584. ISSN: 098-5589.

Iborra, A.; Pastor, J.; Álvarez, B.; Fernández, C. & Fernández-Meroño, J. (2003). Robots in Radioactive Environments, IEEE Journal on Robotics and Automation, vol. 10, num. 4, pp. 12-22. ISSN 1070-9932.

International Maritime Organisation (IMO) (1999). Norm on Hull Integrity. IMO Publishing.

Leveson, N. (1995), Safeware: system safety and computers. ACM Press. ISBN: 0-201-11972-2.

Neumann, P. (1994). Computer-Related Risks. Addison-Wesley Professional. ISBN: 0-201-55805-X.

Stahl, T. & Völter, M. (2006). Model-Driven Software Development: Technology, Engineering, Management. Wiley. ISBN: 0470025700.

Appendix A. Complete Tables

Hazard	Task	Risk Level	Origins	Prob.	Reaction measures
H1. The cleaning tool hits the ship hull.	T5-7, T21	Severe	Breakage or error in the axis controller. Comm. failure (logic or physic)	Low	Emergency alarm[3] Stop axis and move it away from the hull. Power axis off.
H2. Over exposure of the tool or delayed deactivation.	T10	Slight	Breakage of an axis of the secondary positioning system or the tool. Software scheduling error. Communication failure.	Low	Emergency alarm. Power tool off. Stop grit-blasting.
H3. Workers in the trajectory of the primary positioning system (rail).	T1	Very severe	There is a person in the trajectory of the movement of the primary positioning system.	Med.	Emergency alarm. Stop the robot. Emergency stop.
H4. Equipment in the trajectory of the primary positioning system (rail).	T1, T20	Severe	There is an obstacle in the trajectory of the primary positioning system.	Med.	Emergency alarm. Stop the robot. Emergency stop.
H5. Obstacle in the trajectory of the primary (vertical axis or arm).	T2-4, T20	Very severe	There is an obstacle in the trajectory of the primary positioning system.	High	Emergency alarm. Stop the robot. Emergency stop.
H6. Obstacle in the trajectory of the secondary positioning system.	T5-8, T21	Very severe	There is an obstacle in the trajectory of the secondary positioning system.	Low	Emergency alarm. Stop the robot. Emergency stop.
H7. Primary pos. sys. limit sensor overcome (arm).	T3-4, T20	Very severe	Sensor breakage or software error. Comm. failure (either physical or logical).	Low	Emergency alarm. Emergency stop.

[3] Different alarm levels: visual, acoustic, etc, depending on the severity.

Hazard	Task	Risk Level	Origins	Prob.	Reaction measures
H8. Primary pos. sys limit sensor overcome (rail).	T1, T20	Very severe	Sensor breakage or software error. Comm. failure (either physical or logical).	Low	Emergency alarm. Stop the robot. Power axis off.
H9. Secondary pos. sys. limit sensor overcome (arm).	T5-7, T21	Slight	Sensor breakage or software error. Comm. failure (either physical or logical).	Low	Emergency alarm. Stop secondary pos. system. Power secondary off.
H10. The secondary pos. sys. hits the ground or the ship hull.	T1-3, T4,T8 T20	Severe	Sw error when calculating the trajectory of the primary. Human error when moving the primary. Error or breakage of the secondary proximity sensors. Sensor breakage or Sw error. Mechanical failure. Power failure. Comm. failure .	High	Emergency alarm. Emergency stop. Stop secondary and move the arm of the primary. . Power robot off.
H11. The emergency stop does not work.	All	Very severe	Comm. failure . Emergency stop button breakage.	Low	Emergency alarm. Manually power robot off.
H12. The secondary pos. sys. does not stop.	T5-7, T14, T21	Severe	Error in the secondary positioning system controller. Comm. failure (either physical or logical). Power failure.	Low	Emergency alarm. Power robot off. Emergency stop.
H13. The primary pos. sys. does not stop.	T1-4, T8, T12, T13, T20	Very severe	Error in the primary positioning system controller. Comm. failure . Power failure.	Low	Emergency alarm. Power robot off. Emergency stop.
H14. The secondary pos. sys. movement sequence does not end.	T7, T21	Slight	Sw error when controlling the sequence of movements. Comm. failure (either physical or logical).	Low	Emergency alarm. Stop secondary and deactivate blasting tool.

Hazard	Task	Risk Level	Origins	Prob.	Reaction measures
H15. The primary pos. sys. movement sequence does not end.	T8, T12-T13, T20	Very severe	Sw error when controlling the sequence of movements. Comm. failure (either physical or logical).	Low	Emergency alarm. Stop primary axes.
H16. The axis does not get disabled.	T15	Slight	Axis Sw control error.	Low	Emergency alarm. Power robot off. Emergency stop.
H17. The robot does not behave has expected.	All	Very severe	Robot Sw control error. Hw failure. Power failure.	Low	Emergency alarm. Power robot off. Emergency stop.
H18. Free fall of the arm or the vertical axis of the primary.	All	Very severe	Axis controller Hw failure.	Low	Emergency alarm.
H19. Free fall of the secondary.	All	Severe	Axis controller Hw failure.	Low	Emergency alarm.
H20. Grit blasting hose released.	T5-7, T9, T10, T18	Very severe	Hose or connectors broken or hooked.	Med.	Emergency alarm. Emergency stop.
H21. Energy not released in maintenance mode (learning, calibration, etc)	T20-29	Very severe	Mechanical or electrical media necessary to release energy are not implemented correctly.	High	Emergency alarm. Emergency stop.
H22. The tool is activated outside the working area.	All	Severe	Communication failure. Human operator error. Calibration failure. Control Sw failure.	High	Emergency alarm. Emergency stop.
H23. The robot does no exit working mode after alarm.	All	Very severe	Control software failure. Communication failure.	Low	Emergency stop.
H24. Person in the robot working area.	All	Very severe	There is a person in the trajectory of the robot.	High	Stop the system. Emergency stop.

Hazard	Task	Risk Level	Origins	Prob.	Reaction measures
H25. The robot does not stop at operator command.	All	Very severe	Operator fails managing the robot. Control Sw or comm. failure. Hw or mechanical failure.	Low	Emergency alarm. Emergency stop.
H26. Higher parts of the crane oscillate dangerously	All	Very severe	Wind at higher speed that allowed for the crane (50 Km/h). Drastic changes in speed and direction in the movements of the primary. Rails in the primary with dust or strange elements.	Med.	Emergency alarm. Emergency stop.
H27. Irregular movement of the robot.	All	Severe	Dust, grit, humidity, lack of oil, waste of elements.	High	Emergency alarm. Emergency stop.
H28. Some part of the robot (hoses, cables) hooks or falls.	All	Very severe	Bad attachment of cables and hoses.	High	Emergency alarm. Emergency stop.
H29. Dust or grit in the environment.	All	Severe	Another dust generating task taking place near the robot. Bad aspiration of the blast tool. Escapes in connectors or inadequate hoses. Hw, Sw or comm. failure.	High	Take note of the incidence. Cleaning of the environment and the equipment.
H30. Water or humidity in the equipment.	All	Severe	Rain. Proximity of other operations using water.	High	Take note of the incidence. Secure stop of the equipment.
H31. Extreme temperatures over admissible ranges.	All	Severe	Extreme environmental conditions, cold or hot.	High	Take note of the incidence. Secure stop of the equipment.

Table 3. Complete hazard identification list.

Hazard	Risk	SEV. EXP. AV. RRC	Solution	SEV. EXP. AV. RRC
H1. The tool hits the ship hull.	R1. Tool breakage or damage to the secondary positioning system.	S1 E2 A1 R3A	Add bumpers to the head of the tool. Limit Z-axis maximum torque.	E1 A1 S1 R4
H2. Overexposure of the tool or delay in its deactivation.	R2. Damage to the ship hull surface.	S1 E2 A1 R3A	Add a software timer to control the tool working time. Add a motion sensor to the secondary positioning system and link it to the timer.	E1 A1 S1 R4
H3. Workers in the trajectory of the primary positioning system (rail).	R3. Worker runs over.	S2 E2 A1 R2A	Add sensors to detect obstacle presence in the rail. These sensors are directly wired to the robot safety control infrastructure. Add a siren for signalling robot motion.	E1 A1 S2 R3B
H4. Equipment in the trajectory of the primary positioning system (rail).	R4. Damage to the equipment and to the primary positioning system.	S2 E2 A1 R2A	Same as H3	E1 A1 S2 R3B
H5. Obstacle in the trajectory of the primary (vertical axis or arm)	R5. Damage to the primary and to the obstacle	S2 E2 A2 R1	Add sensors for detecting obstacles in the trajectory of the arm and wire them to the robot safety control infrastructure.	E1 A1 S2 R3B
H6. Obstacle in the trajectory of the secondary pos. sys.	R6. Damage to the secondary or to the tool	S2 E1 A1 R2B	Hw/Sw torque control for detecting overload.	E1 A1 S1 R4
H7. Primary pos. sys. limit sensor overcome (arm).	R7. Damage to the primary pos. sys. and/or workers.	S2 E1 A2 R2B	Add mechanical limits	E1 A1 S1 R4
H8. Primary pos. sys limit sensor overcome (rail).	R8. Damage to the primary positioning system and/or workers or equipment.	S2 E1 A2 R2B	Add mechanical limits	E1 A1 S1 R4

Hazard	Risk	SEV. EXP. AV. RRC	Solution	SEV. EXP. AV. RRC
H9. Secondary pos. sys. limit sensor overcome (arm).	R9. Damage to the secondary positioning system.	S1 E1 A2 R3B	Add mechanical limits	E1 A1 S1 R4
H10. The secondary pos. sys. hits the ground or the ship hull.	R10. Damage to the secondary positioning system and/or workers or equipment.	S2 E2 A2 R1	Define a precise procedure for positioning tool over hull surface. Add proximity sensors to the secondary (XYZ table), monitorised by control system.	E1 A1 S2 R3B
H11. The emergency stop does not work.	R8. Damage to the primary positioning system and/or workers or equipment.	S2 E1 A2 R2B	Physical redundancy of the emergency stop system.	E1 A1 S1 R4
H12. The secondary pos. sys. does not stop.	R11. Secondary positioning system breakage.	S1 E1 A2 R3B	Add additional emergency stop mechanisms. Add external motion sensors.	E1 A1 S1 R4
H13. The primary pos. sys. does not stop.	R8. Damage to the primary positioning system and/or workers or equipment.	S2 E1 A2 R2B	Add additional emergency stop mechanisms Add external motion sensors (6.4 ANSI).	E1 A1 S1 R4
H14. The secondary pos. sys. movement sequence does not end.	R12: The robot moves uncontrolled	S1 E1 A1 R4	Add a software module for monitoring the execution of the sequence.	E1 A1 S1 R4
H15. The primary pos. sys. movement sequence does not end.	R8: Robot knocks over	S2 E1 A1 R2B	Add emergency stop mechanisms Add motion sensors outside the control loop Add sensor to measure the crane slope. Stop system is slope surpasses a threshold.	E1 A1 S1 R4
H16. The joint does not get disabled.	R13: Damage to the joint.	S1 E1 A1 R4	Add current sensor to detect joint enable state. Add alarm to inform operator.	E1 A1 S1 R4

Hazard	Risk	SEV. EXP. AV. RRC	Solution	SEV. EXP. AV. RRC
H17. The robot does not behave has expected.	R14. Damage to environment, equipment or workers.	S2 E1 A2 R2B	Add mode constraints verification measures (commands allowed, max speed and acceleration, …) in control software.	E1 A1 S1 R4
H18. Free fall of the arm or the vertical joint of the primary.	R14. Damage to environment, equipment or workers.	S2 E1 A2 R2B	Add safety brake (stops joint in case of power failure). Add anti-fall mechanism (block stop) to vertical joint.	E1 A1 S2 R3B
H19. Free fall of the secondary.	R14. Damage to environment, equipment or workers.	S2 E1 A2 R2B	Add safety brake (stops joint in case of power failure).	E1 A1 S1 R4
H20. Grit blasting hose released.	R14. Damage to environment, equipment or workers.	S2 E2 A2 R1	Add sensors to detect hose release. Identify hoses and nozzles by means of codes of colors.	E1 A1 S2 R3B
H21. Energy not released in maintenance mode (learning, calibration, etc)	R14. Damage to environment, equipment or workers.	S2 E1 A2 R2B	Add means to discharge stored static electricity. Use proper earth connections and test them before operation. Use adequate protections against electrical risk. Limit robot speed in maintenance or programming modes.	E1 A1 S2 R3B
H22. The tool is activated outside the working area.	R14. Damage to environment, equipment or workers.	S2 E1 A2 R2B	Add mode constraints verification measures (tool activation…) in control software.	E1 A1 S1 R4
H23. The robot does no exit working-mode after alarm.	R14. Damage to environment, equipment or workers.	S2 E1 A2 R2B	Add redundancy: independent module to process alarms and start safety actions. Add means to coordinate control system and alarm processing module. Control system and alarm processing module should be aware of their respective behaviors and stop the system if detect a failure in the other.	E1 A1 S1 R4

Hazard	Risk	SEV. EXP. AV. RRC	Solution	SEV. EXP. AV. RRC
H24. Person in the robot working area.	R15: Damage to people due to mechanical parts or grit impact.	S2 E1 A1 R2B	Mark working area. Identify hoses and nozzles by means of codes of colors. Add sensors to detect obstacle presence in the rail. Add a siren for signalling robot motion.	E1 A1 S1 R3B
H25. The robot does not stop at operator command.	R14. Damage to environment, equipment or workers.	S2 E1 A2 R2B	Add emergency stop mechanisms. Add redundancy: independent module to process alarms and start safety actions.	E1 A1 S1 R4
H26. Higher parts of the crane oscillate dangerously	R8: Robot knocks over R14. Damage to environment, equipment or workers.	S2 E2 A2 R1	Add motion constraint: horizontal movements over rails should be done with secondary in lower position. Add sensor to measure wind speed. Add sensor to measure the crane slope. Stop system is slope surpasses a threshold.	E1 A1 S1 R4
H27. Irregular movement of the robot.	R15: Breakage of joints mechanical parts. R16: Vibrations cause Hw breakage or malfunctioning.	S1 E2 A1 R3A	Periodical maintenance. Cleaning of equipment after working. Add sensor to measure the crane slope. Stop system is slope surpasses a threshold.	E1 A1 S1 R4
H28. Some part of the robot (hoses, cables) hooks or falls.	R8: Robot knocks over. R17: Hoses and wire breakage. R15: Damage to people due to mechanical parts or grit impact.	S2 E1 A2 R2B	Add emergency stop mechanisms. Plug and fix properly hoses and wires. Inspect working area.	E1 A1 S1 R3B
H29. Dust or grit in the environment.	R15: Damage to people due to mechanical parts or grit impact. R18: Damage to spotlights. R19: Vision system malfunctioning.	S2 E2 A2 R1	Plug and fix properly hoses and wires. Use dust-resistant spotlights and protect them. Protect video cameras.	E1 A1 S1 R3B

Hazard	Risk	SEV. EXP. AV. RRC	Solution	SEV. EXP. AV. RRC
H30. Water or humidity in the equipment.	R19: Vision system malfunctioning. R20: Electrical shortcut. R21: spotlights explosion.	S2 E2 A2 R1	Use water-resistant connectors. Use dust-resistant spotlights and protect them. Use water resistant video cameras.	E1 A1 S1 R3B
H31. Extreme temperatures over admissible ranges.	R22: Hoses freezing. R23: Hw breakage or malfunctioning.	S1 E1 A2 R3B	Add temperature sensor. Add ventilation to drivers and hardware devices.	E1 A1 S1 R4

Table 4. Complete hazard identification list.