Grant agreement no: FP7-600877

SPENCER:

Social situation-aware perception and action for cognitive robots

Project start: April 1, 2013

Duration: 3 years

DELIVERABLE 6.6

Safety Audit (Supplementary Report)

Due date: month 19 (October 2014)

Lead contractor organization: BLUE

Dissemination Level: PUBLIC

Contents

Abstract

This report documents on the tests and measures undertaken by the SPENCER consortium to provide a formal analysis of the potential failure modes of the robot platform used in the project. To do this, we utilize an established method called Failure Mode and Effects Analysis (FMEA). The result of this analysis as well as the consequential safety measures that we have taken are given in this report.

1 Introduction

During Integration Week II in Toulouse, representatives of the four partners BLUE, CNRS, ALU-FR, and TUM performed a formal analysis of the safety aspects of the SPENCER robot platform. The major part of this was the application of a Failure Mode and Effects Analysis as explained in the next section. Furthermore, BLUE performed a thorough analysis of the usefulness of the bumpers (see Sec. 3), and we established immediate measures to take for an improved safety. Details are given in Sec. 4.

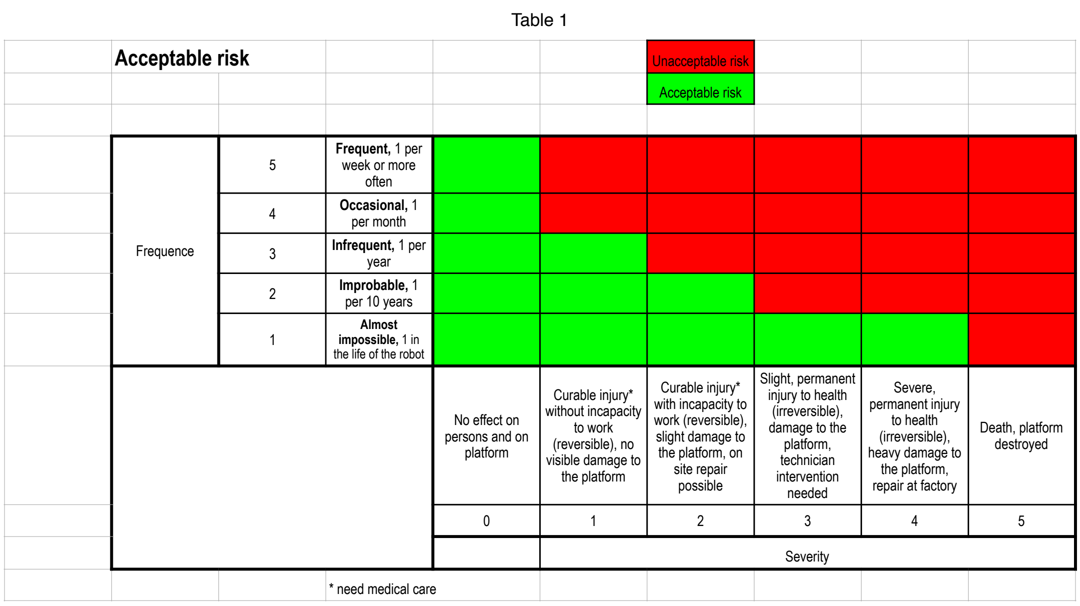

Figure 1: Frequency / risk table. All potentially occuring failure cases are classified into the 5 frequency and the 5 severity classes as specified in the table. From the combination of severity and frequency, an acceptability of the incurred risk is derived: red boxes denote unacceptable risks, green boxes represent acceptable risks.

2 Failure Mode and Effects Analysis

The Failure Mode and Effects Analysis (FMEA) is a formal tool to determine potential issues with respect to the safety of a given system, in our case the mobile robot platform, and to find measures to solve these issues. The main steps of this analysis are a component-wise listing of all potential failure modes, an assignment of severity and frequency levels for each such failure mode, and the determination of actions to solve each failure mode. The result of the FMEA performed for the SPENCER platform is shown in the appendix. In addition, we also provide a list of "What-if" questions in table 1, which gives a more natural summary. However, we note that the formal FMEA sheet in the appendix is more detailed and should be used for reference. It also provides a quantification of the different failure modes based on the different levels of severity and frequency as given in Fig. 1. Here, we see the 5 different levels we defined both for severity and for frequency. We also classified each failure mode into "acceptable risk" and "unacceptable risk", and this classification was done based on the combination of frequency and severity as also shown in Fig. 1 where red cells correspond to unacceptable risks and green cells to acceptable risks.

A summary interpretation of the resulting FMEA table (see appendix) is given as follows:

- Most failure modes have acceptable risks, either because their severity is comparably low or because they occur too seldom to be considered as unacceptable.
- The failure modes to which we assigned an unacceptable risk mainly concern higher-level software components and much less the low-level components. This means that, as long as the low-level components including the sensors, the actuators, and the collision avoidance module work reliably, many failures of the higher level components can be handeled.
- In particular, stairs and overhanging obstacles above the laser plane are hard to detect. The current solution to this problem is to restrict the access to certain areas by annotating them in the map (defining "no-go areas"). Furthermore, and most importantly, the robot is equipped with a *remote switch*, a safety-certified radio emergence button to stop the robot.

In general we note that the last resort for any kind of failure case are the emergency stop buttons on the platform and the certified remote button, by which the platform can be stopped immediately at any time. This remote emergency stop button is held by a dedicated person, who is instructed to always maintain a free sight to the platform and the environment in immediate vicinity of the robot. Also, this person must not be distracted by other tasks or by other people, e.g. having conversations during operation. Thus, technically the person holding the certified remote emergency button can be seen to be the *driver* of the platform.

In addition to this important safety component, we established more measures as we want to reduce the need for intervention of the operator without sacrificing safety, described in Sec. 4.

3 Analysis of the Bumpers

In addition to the general FMEA, we particularly analysed the usefulness of the bumpers on the robot platform. The spread sheet used in this analysis is given in Fig. 2. From the measures given in

Question	Answer
What happens if the robot batteries run empty?	ANT system detects low battery level and stops robot
What if, prior to that, the laptops run out of battery (e.g. because they are not properly powered from robot)?	ANT watchdog detects communication problem, robot is stopped
What if any of the robot PCs crashes / freezes? Or a laptop?	ANT watchdog detects communication problem, robot is stopped
What if any of the sensor cables comes loose while moving, or is not properly connected while e.g. inserting the laptops?	Laser communication is checked by ANT, robot is stopped if laser sends no data
What if one of the wheel encoder cables comes loose or breaks?	Failback mechanism implemented in ROS, checks if wheel encoder values don't change although the robot should be moving; if yes it sends an emergency stop command
What if any of the software components responsible for obstacle avoidance crashes?	If no commands are sent, the driving safeguard stops the robot after 100 ms. If wrong commands are sent robot is stopped remotely.
What if localization fails?	The driving safeguard checks for big jumps in motion commands and limits velocity.
How does the robot detect obstacles below laser height, such as very small children?	Currently, no detection below laser plane. Robot is stopped remotely. An RGB-D based collision checker is under development.
How does the robot avoid driving onto stairs (esp. with negative inclination) and escalators?	The stairs will be marked in the map. If robot still approaches stairs, remote emergency button will be pressed.
How to prevent the robot from driving onto horizontal escalators (moving sidewalks)?	Same as stairs.
How does the robot detect and avoid driving into glass surfaces (e.g. the elevators)?	Same as stairs.
Can children climb onto the robot's base? Will the robot still drive?	Collision checker detects children and stops robot. If not, the robot will be stopped remotely.
Can the robot fall over by pushing it or climbing onto it?	No, the center of gravity is low enough.
Is it possible to spill liquids into the robot, possibly causing an electrical short?	Main fuse burns. Computers can be damaged.
Who takes over the responsibility of operating the wireless emergency stop?	A dedicated person who is sufficiently instructed and must not be distracted.

Table 1: "What-if" questions.

Table 1

Bumper analysis

Limitation of efforts and of energy		
Max pressure	50	N/cm
Max effort	150	N/cm2
Max Kinetic energy	10	J
Energy		
Plaftom weight	250	kg
V_{max}	1.8	m/s
E_{cin} at V	**405**	**J**
V @E_{cin}	**0.282842712**	**m/s**
Force		
Motor max continuous torque	8	Nm
Motor max peak torque	24	Nm
Wheel diameter	0.31	mm
Continuous force	**103.2258064**	**N**
Peak force	**309.6774193**	**N**
Pressure		
Case: 1 leg blocked between the platform and a wall		
contact surface (20x5 cm)	100	cm
Continuous pressure	**1.032258064**	**N/cm**
Peak pressure	**3.096774193**	**N/cm**

Energy		
Plaftom weigh	130	kg
V_{max}	1.8	m/s
E_{cin}	**210.6**	**J**
V @E	**0.392232270**	**m/s**

Conclusion

Pressure applied by the bumper on the body is acceptable.

Bumper is useful if the speed of the platform is < 0.28 m/s.

If 60 kg of battery is removed, a speed of 0.32 m/s is acceptable.

force is not relevant, because of the big surface of the bumpers.

Figure 2: Analysis of the bumpers

the table, it resulted a speed of maximal $0.28m/s$ at which a safe operation of the bumpers can be guaranteed. Furthermore, the potential pressure applied to an object or a human leg that is blocked between the platform and a wall is given and classified as “acceptable”, as it is comparably low. To verify this, we performed a test where the robot collided with a human who was standing in front of a wall. As determined by the calculations, the resulting pressure was low enough to not cause any injuries.

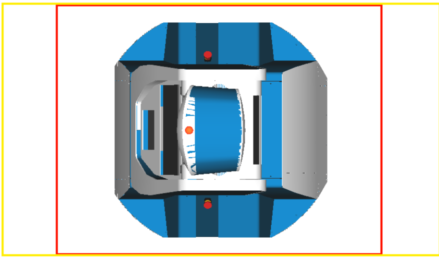

Figure 3: Safety zones of the collision checker around the SPENCER robot. Error zone in red, warning zone in yellow.

4 Immediate Safety Measures

As an outcome of the FMEA performed at the Integration Meeting, the following immediate measures have been taken and will be taken in our future work:

- We implemented and tested a **collision checker** which acts as a "virtual bumper". This module is also described in deliverables D5.3 and D6.2). It consists of two ROS-based software components, a laser-based *low-level obstacle detection* module and a *driving safeguard*. The former module detects any obstacles at laser height within a "warning zone" and an "error zone":
  - When an obstacle is detected in the warning zone, which starts at 60 cm in front of the robot (in its direction of travel) and 20 cm to the sides, the linear velocity of the robot is limited to at most 0.3 m/s by the driving safeguard (see Fig. 3). The angular velocity is scaled down accordingly.
  - The error zone begins at 35 cm in front of and 3 cm to the sides of the robot, and prohibits any motion. Movement in backwards direction is still allowed if the rear is clear, and vice versa. Sharp turning on the spot is only allowed if both front and rear are clear.

  The mentioned parameters are still subject to additional fine-tuning. The reaction time of the system was estimated in experiments to be around 50–100 ms.

  The *driving safeguard* also monitors for timeouts of the collision status or velocity commands, and prompts for the robot to stop immediately in case a timeout occurs. Lastly, any high-level component running on the SPENCER robot platform can ask the driving safeguard to trigger a "software emergency stop" in case something unexpected happens. The software emergency stop status bit has to be cleared explicitly by user input before any further drive motion can be executed.

- The integration of an RGB-D-based obstacle detection module to also detect obstacles at or below laser height is planned. It is supposed to function in a similar fashion, with a warning and an error zone. This is on-going work and we expect a collision checker based on 3D-data to be operational in Integration Week IV at the latest.

- Braking tests were performed during the Integration Meeting, by placing an obstacle in front of the robot platform at laser height as well as by manual triggering via the wireless emergency stop. An example of such a braking test can be seen in a video on the web site of SPENCER (see http://spencer.eu/videos/braking_test1.mp4). The braking distance of the robot was found to be currently too long (20–40 cm) at velocities higher than 0.7 m/s which is due to a too shallow deceleration ramp configured in the motor controllers. This configuration will be changed so that a faster braking maneuver can be performed. We will address this for the next Integration Week III where we will repeat the breaking tests with the modified deceleration ramps.

- As a further measurement, we are considering the necessity to increase the thickness of the foam layer on the bumpers if we have evidence to do that from some additional brake tests.

5 Conclusions

We performed a detailed analysis of the potential failure cases of the robot platform, as well as their potential impacts and possible measures to mitigate them. Apart from the safety-certified remote button, which is already an integral component by which the robot can be stopped at any time, we established several immediate safety measures, which have already been or are being implemented. The on-going measures are an extended collision checker based on 3D data from a forward-looking RGB-D sensor and better configurations of the drive motor controllers that allow for steeper deceleration ramps. Both measures will be implemented and tested during Integration Weeks III and IV, respectively.

Appendix: FMEA Table

The FMEA sheet used for this safety audit is shown on the following pages.

Component/ functionality	Potential failure mode	Potential failure cause	Potential failure effect	Severity	Frequency	Current measure	Detection ranking	RPN	Recommended action	To be documented
"SPENCER Software" in general	Bad command sent to the ANT box	- Computation failure - Bug in software	Wrong movement of platfrom, potential collision	4	5	- Bumper to stop robot in case of collision at bumper level - Press wireless E-stop button - Press E-stop button	2	40	Analyze bumper efficiency	Indicate in the user manual that: 1) New software must be validated in safe unpopulated area 2) Test in populated area must be done with validated software
	Stairs not detected	- Perception problem - Bug in software	Robot falls into the stairs, potentially crushing people	5	3	-Press wireless E-stop - Press E-stop button	2	30		Indicate in the user manual that the robot has no fall protection sensor. Before deployment in populated area, check for stairs and protect them
	Obstacle at height of bumpers not detected by sensors	- Perception problem - Bug in software	Potential collision	4	5	- Bumper to stop robot in case of collision - Press wireless E-stop button - Press E-stop button	2	40	Analyze bumper efficiency	Indicate in the user manual that objects out of laser scanner plane will not be detected
	Obstacles above bumpers not detected by sensors	- Perception problem - Bug in software	Potential collision	4	5	- Press wireless E-stop - Press E-stop button	2	40		Indicate in user manual that obstacles above the bumper wll not be detected
	Movement command sent during charging	- Bug in software - Bad manipulation	Safety loop opened when charger plugger in platform (door open), platform doesn't move	0	4		1	0		Ask user to check that when the door is open, the safety LED is ON
	Communication problem with ANT	- Cable broken - Network problem - Software problem	Watchdog in communication, problem detected by ANT, safety loop opens	0	4		1	0		
Motion controllers	Wrong command executed by the motor	- Controller crash - Hardware failure	ANT detects odometry issue, ANT ok signal opens safety loop	0	3		1	0		
	Do not activate brake when commanded	- Controller crash - Hardware failure	Commanded speed= 0, the motor stops	0	3		1	0		
	Wrong command and brake not activated	- Controller crash - Hardware failure	Robot turns on itself, potential risk of collision	2	2		10	40		
	Wrong command and brake not activated on both motors	- 2x controller crash - Hardware failure	Wrong movement of platfrom, potential collision	4	1		10	40		
	CAN communication not working	- Cable broken	CAN issue detected by ANT, ANT ok signal opens the safety loop	0	2		1	0		
ANT lite	Bad command sent to the motor controllers	- Bug in ANT software - Hardware failure	Wrong movement of platfrom, potential collision	4	2	- Bumper to stop robot in case of collision - Press wireless E-stop button - Press E-stop button	4	32	Analyze bumper efficiency	
	ANT ok signal not activated	- Bug in ANT software - Hardware failure	Safety loop not activated, potential collision	4	1		10	40		
Sick scanners	Bad communication with the ANT box	- Scanner problem - cable broken - perturbations	Communication issue detected by ANT, ANT ok signal opens the safety	0	3		1	0		
	Bad information sent by scanner	- Internal scanner failure	Potential wrong movement of the platform, potential collision	4	1		5	20		
Wireless E-stop	Device not working	- Failure of device	Ple D, SIL 2, safety components, the safety loop is opened	0	1		1	0		
	Remote control out of range	- Operator too far from robot	Distance remote-device monitored, the safety loop is opened	0	5		1	0		
Safety loop	Any relay blocked open	- Failure of a relay	Safety loop opened	0	2		1	0		
	Any relay blocked closed	- Failure of a relay	Redundancy, safety loop opens, platform won't move	0	2		2	0		Regularly check that both relays are properly working (by inspecting LEDs) to ensure redundancy, document in manual
	E-stop button does not open safety line	- Switch failure	Redundancy, safety loop opens, platform won't move	0	2		2	0		
		- Emergency stop button failure	Platform does not stop, potential collision	4	2	- Bumper to stop robot in case of collision - Press wireless E-stop button - Press E-stop button	2	16	Analyze bumper efficiency	
	Door closed not detected	- Cable broken - Switch broken (open)	Safety loop open, platform won't start	0	2		1	0		
	Door open not detected	- Cable short circuit	redundancy, safety loop opens, platform won't move	0	2		1	0		
		- Switch broken (closed)	Door open not detected, platform may move with door open	2	2		1	4		Ask user to check that when the door is open, the safety LED is ON
Bumper	Bumper pressed not detected	- Cable broken	NC circuit, bumper considered pressed, redundancy 2 cables, safety loop opened	0	2		1	0		
	Bumper pressed not detected	- Switch broken in open position	NC circuit, bumper considered pressed, redundancy 2 cables, safety loop opened	0	2		1	0		
	Bumper pressed not detected	- Switch blocked/ broken in closed position	Platform do not stop, potential collision	4	2	- Press wireless E-stop button - Press other E-stop button	2	16	Analyze bumper efficiency	Ask user to check the bumpers at start-up
	Bumper not detecting obstacle	- Obstacle too light	Collision with obstacle	4	2	- Press wireless E-stop button - Press E-stop button	2	16		
Power supplies	Line touching the chassis	- Broken cable	Short circuit, the internal protection of power supplies cuts power	0	2		5	0		
Cabling	24V touching chassis	- Broken cable	main fuse burn!	1	2		5	10		
Batteries	Batteries empty when robot in movement	- Not being recharged	ANT detects battery level, first gives a warning, then ANT ok signals opens the safety loop	0	4		10	0		
	Some battery connectors unplugged	- Human error	Still 24V available but 1/2 capacity	0	3		5	0		
	All batteries not connected	- Human error	Only 12V avalable, ANT detects battery low, ANT ok signals open the safety	0	3		5	0		

Stability	Vehicle tilting	- High speed in a curve	Platform does not tilt, gravity center low enough.	4	1	- Obstacle avoidance will decrease speed if obstacles in surroundings	5	20	Curve at high speed to be tested in secured area. If test fails, then reduce maximum allowed speed	
	Vehicle tilting	- Powerful brake during emergency stop	Platform does not tilt, gravity center low enough.	4	1	- Obstacle avoidance will decrease speed if obstacles in surroundings	5	20	Emergency stop to be tested at maximum speed in secured area. If test fails, reduce the maximum allowed speed	
	Vehicle tilting	- Steep slope	Potential tilting	5	3	- Block robot from excessive slopes - Emergency stop buttons	1	15		Document maximum allowed slope that the platform can drive upon
	Vehicle tilting	- Someone pushing or pulling the platform	Platform will tilt but not fall, gravity center too low	3	2	- The person with the wireless emergency stop button must stop this action	1	6		
People	Child on the platform	- Children climbing the platform	Obstacle seen by laser scanner, platform do not move	0	3	- The person with the wireless emergency stop must remove the child	10	0		
	Liquid in the platform	- Liquid spilled by someone	Short circuit in the electrical circuit, Main fuse burns Laptop can be destroyed	1	4		5	20		
Driving safeguard (ROS)	Does not receive commands from planner	- Motion planner crash - Software bug - Network problem	Driving safeguard detects timeout after 100 ms, speed commands are set to 0. The platform stops within the braking distance.	0	5		1	0		
	Receives wrong commands from planner	- Planning failure - Software bug - Network problem	Low risk of collision due to low-level obstacle collection still being active	2	5	- Obstacle detection to stop the robot - Bumper to stop the robot - Press wireless E-stop button - Press E-stop button	2	20		Operator with wireless E-stop must closely monitor the robot's behavior, especially in the vicinity of humans
	Sends bad commands	- Software bug in driving safeguard	Potential collision	4	3	- Bumper to stop the robot in case of collision at bumper level - Press wireless E-stop button - Press E-stop button	2	24	Thorough software testing (also in simulation) and code reviews, keep code as simplistic as possible	Operator with wireless E-stop must closely monitor the robot's behavior, especially in the vicinity of humans
	Sends no commands	- Crash of driving safeguard	Potential collision, but ANT watchdog will detect timeout after 100 ms. The platform stops within the braking distance.	0	4	- Obstacle detection to stop the robot - Bumper to stop the robot in case of collision at bumper level - Press wireless E-stop button - Press E-stop button	1	0	Verify that ANT watchdog is activated properly by killing driving safeguard on purpose.	
Obstacle detection (ROS)	Does not receive sensor input	- Network issue - Laser driver crashed	Stops sending obstacle status messages. Driving safeguard detects timeout after 100 ms, speed commands are set to 0. The platform stops within the braking distance.	0	3		1	0		
	Sends wrong obstacle status messages	- Software bug	Potential collision	4	3	- Bumper to stop the robot in case of collision at bumper level - Press wireless E-stop button before collision - Press E-stop button	3	36	Thorough software testing (also in simulation) and code reviews, keep code as simplistic as possible	
	Sends no obstacle status messages	- Crash - Software bug - Missing sensor input	Driving safeguard detects timeout after 100 ms, speed commands are set to 0. The platform stops within the braking distance.	0	3		1	0		
	Does not detect obstacles	- Obstacle below or above laser plane	Potential collision	4	5	- Bumper to stop the robot in case of collision at bumper level - Press wireless E-stop button before collision - Press E-stop button	3	60	Implement RGB-D collision checker that also sees obstacles below and above laser plane	Operator with wireless E-stop must always watch out for obstacles that the laser might not see (children or luggage on the floor, information screens mounted above laser height, etc.)