Ref. Ares(2022)4750815 - 29/06/2022

REMODEL - Robotic tEchnologies for the Manipulation of cOmplex DeformablE Linear objects

Deliverable 2.6 – Report on the robot safety tests

Version 2022-06-28

Project acronym: REMODEL
Project title: Robotic tEchnologies for the Manipulation of cOmplex DeformablE Linear objects
Grant Agreement No.: 870133
ObjectsTopic: DT-FOF-12-2019
Call Identifier: H2020-NMBP-TR-IND-2018-2020
Type of Action: RIA
Project duration: 48 months
Project start date: 01/11/2019
Work Package: WP2
Lead Beneficiary: TAU
Authors: TAU, TECNALIA, ELIMCO, PUT
Dissemination level: Confidential
Contractual delivery date: 30/06/2022
Actual delivery date: 29-06-2022
Project website address: https://remodel-project.eu/

Table of contents

1. Scope

The tasks T2.4 (Risk assessment and safety requirements) and T2.5 (Safety implementation, testing and evaluation) formed the basis of determining the various requirement of safety for the individual use cases (at various levels of implementation) and the actual implementation of a hardware and software based solution for device and system safety, respectively. The task for Risk assessment and safety requirements was active from M1 – M5, however, the document is still being updated by the partners to maintain an up-to-date document for system safety requirements; and the task for Safety implementation, testing and evaluation has been active for several months at various TRL levels, and is currently at TRL5 (began at TRL 3).

The Deliverable D2.6 aims to document the safety strategies and protocols implemented by the REMODEL consortium (so far), to have a generic approach to utilize safety devices, create safety logics, setup inter-modular communication, and visualize the system (safety) status to the human user.

The safety devices considered and utilized, differ between the individual use case implementations, as the nature of robotic systems vary (industrial robot and cobots). This greatly impacts the selection of the safety system hardware and controller, and the nature of the logics implemented. The REMODEL Safety Manager (RSM) was the dedicated ROS based module developed for the project, and is expected to be exploited across most of the use cases to manage the platform's physical safety and integrate the safety system into the REMODEL system architecture.

The structure of the document is as follows: In Section 2 the safety architecture and the RSM module are explained in detail for a generic implementation, highlighting the various functionalities and communication aspects. Then, in Section 3 the safety systems' requirements, development, and utilization of two of the REMODEL test beds and the physical tests performed to verify the working are also described. These two test beds represent how safety can be implemented using the REMODEL safety structure both for an industrial robot cell, and for a fenceless collaborative robot platform. Finally, Section 4 reports the conclusions of the deliverable.

2. Safety architecture

All the use cases of the project, except UC3 (wiring harness assembly) due to the internal policies of Volkswagen (VW), have a common safety architecture. This architecture is generic, so it can adapt to the requirements of the different use cases, and it is composed by the following elements (see Figure 1):

- **Physical safety devices:** Such as emergency stop buttons, light curtains, door switches or laser scanners, depending on the safety requirements of each use case.
- **Safety PLC:** Responsible for the fast and reliable emergency stop of the platform. It receives the signals from the safety devices, stopping the robotic platform immediately if a risk situation is detected. Additionally, it communicates with the ROS system through the RSM updating the safety status.
- **REMODEL Safety Manager (RSM):** ROS node that acts as an intermediary between the physical safety devices and the rest of the modules of the ROS system. This node doesn't need to be that fast and reliable as it is not in charge of stopping the platform. It receives the active alarms and the safety status from the safety PLC and communicates it to the rest of the modules of the ROS system. Additionally, the communication can happen also in the opposite direction, informing the safety PLC about an error or a risk situation detected by the ROS system, in order to stop the platform.
- **ROS system:** The operation of some ROS modules depends on the safety status of the platform, that is published in ROS topics by the RSM. For instance, the planner will stop executing motion commands when there is an alarm and the platform has been stopped, or will modify the speed of a cobot if there is an operator near it. Another ROS module that uses this information is the user interface, that show the active alarms and the safety status, and contains an emergency stop button (not as fast as the physical one) and a reset button to clear the errors (this option is just active in some use cases).

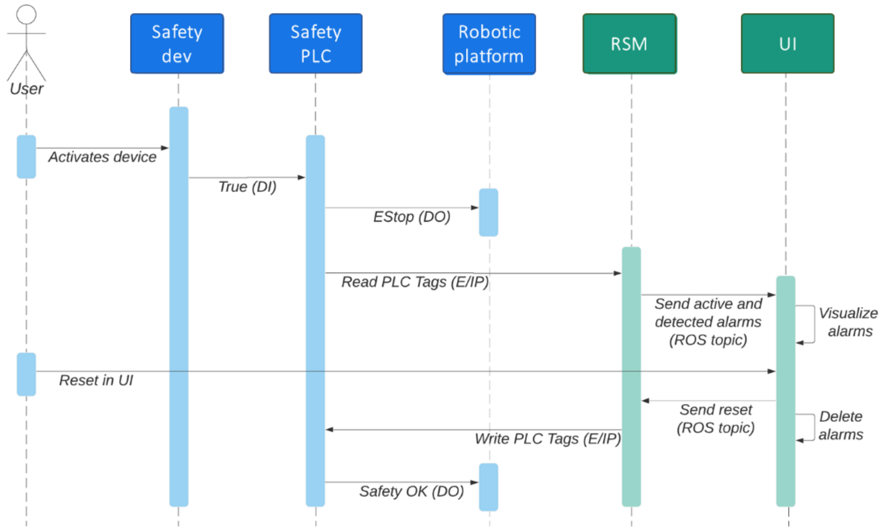

Figure 1. UML sequence diagram of the REMODEL safety system. The blocks in blue are physical devices and the blocks in green are ROS modules. In this figure two examples of communication are shown. In the first one, a safety device (e.g., light curtain) is activated and the signal is propagated; the safety PLC performs the emergency stop of the robotic platform and updates the safety status to the RSM, that publish this information in the ROS system, so the UI can display the alarm. In the second, the communication happens in the opposite direction, so the reset signal of the UI is received by the RSM, that sends this information to the safety PLC.

As mentioned previously, UC3 is an exception, and it doesn't utilize the REMODEL safety architecture, nor the RSM. The reason of this is that all Volkswagen factories all over the world use the same system (scheme - standard), which makes that every maintenance worker is familiar with how the factory works wherever he goes. Regarding safety, all the systems used by VW meet the safety requirements set out in legal regulations and standards. Therefore, as the final robotic platform is planned to work in the future in the factory, in a real production system, it was decided to accept the VW standard and replace RSM in favor of a preparation for the safety systems that Volkswagen uses.

2.1. REMODEL Safety Manager (RSM)

The RSM is the ROS node in charge of managing the safety of the REMODEL robotic platforms, and it allows the bidirectional communication between the physical safety devices and the rest of the modules of the ROS system. This node has a generic structure to be able to be integrated into the different use cases. The node is composed of five steps that are executed cyclically every 100ms. The cycle frequency is not extremely fast as the emergency stop of the system is managed by the safety PLC and the function of the RSM is just informing about the safety status to the rest of the system.

1. **Read safety PLC variables:** Different libraries and communication protocols are used to establish the RSM-PLC communication depending on the PLC branch and model selected for each use case.
2. **Update ROS safety information:** The safety information published by any ROS node of the system is read by the RSM using ROS subscribers. To synchronize this information, the RSM variables are updated with the new data received by the subscribers, in the execution cycle (every 100ms). An example of this ROS safety information are the reset and emergency stop signals published in ROS topics by the user interface.
3. **Data processing:** The received data is processed, determining what has changed from the last cycle and needs to be published or written in the PLC. Additionally, the alarms can be in three states: active, detected (when it is not active, but the system hasn't been reset yet), and safe, being this step responsible for updating the state of each alarm. This step manages also the alarms clearing when the reset button is pressed.
4. **Publish updated safety information:** Once the RSM determines what information needs to be published, it is published in the required ROS topics, so the rest of the ROS modules receive the updated safety information. An example of this is the user interface, which receives the updated state of the alarms and the updated overall safety status and displays it so the operator can see what is wrong (see Figure 2).
5. **Write safety PLC variables:** As in the first step, the implementation of the RSM-PLC communication will depend on the selected devices. This allows also to send information from ROS to the safety PLC, stopping the platform or resetting the alarms with a signal coming from ROS. This functionality is just active in use cases working with collaborative robots.

Figure 2. REMODEL user interface showing the active alarms.

3. SAFETY REQUIREMENTS IMPLEMENTATION AND TESTING

This section documents the various safety equipment used across the different systems, the reasoning for the implementation and its operation. To avoid repeating information, the deliverable focus on two use cases, to show how safety could be implemented in an industrial robotic cell, or in a fenceless collaborative robot platform, using the REMODEL safety architecture. Additionally, this section also highlights the strategy used for evaluating risks from another deliverable made for the same project.

The outcome of **D2.4- Risk assessment, safety requirements and measures**, has highlighted certain medium and high level risks which can be expected to occur while the robotic platform is in operation (either while in the training/ testing phase or in the production phase). The principle behind identifying, evaluating and mitigating the various risks to personnel and equipment (as detailed in D2.4) is highlighted below.

A risk analysis comprises the assessment of what might cause harm to personnel and decide the actions to prevent that harm. After this initial risk identification, it is necessary to score and prioritize them, putting in place appropriate and sensible control measures. The risk analysis should cover all people who might be affected and consider all significant risks in mounting and operation situations. Once the analysis is performed and the appropriate control actions have been decided, only low-level risks will remain.

The risk analysis carried out in task T2.4 is covering the installation and operation of the testbeds at the various stages of evolution of the use cases (TRL 4 to TRL 6).

Table 1 summarizes the risk rating of the assessment. The rating determines the risk level based on the likelihood of an event occurring and the severity of the damage to personnel and equipment that may cause this event. The likelihood ranges from **most unlikely** to ***most likely*** while the severity vary between ***slight*** to ***major injuries***.

Risk Assessment		Severity of Injuries			
		Slight (1) (Injuries that could be treated by the local First Aider form the First Aid Box)	**Minor (2)** (Injuries that may require more expert treatment, administered at a sick bay or out-patients)	**Serious (3)** (Chronic conditions or injuries involving urgent hospital treatment)	**Major (4)** (Injuries involving manor trauma or death)
Likelihood of Injuries	**Most Unlikely (1)** Probability close to zero	Low (1)	Low (2)	Medium-Low (3)	Medium-Low (4)
	Unlikely (2) (Injuries possible)	Low (2)	Medium-Low (4)	Medium-High (6)	Medium-High (8)
	Likely (3) (Injuries highly possible)	Medium-Low (3)	Medium-High (6)	Medium-High (9)	High (12)
	Most likely (4) (Injuries probable)	Medium-Low (4)	Medium-High (8)	High (12)	High (16)

Table 1 - Risk rating

Based on the rating obtained by each identified risk, remedial actions might be required to reduce their level and maintain the risks at minimum. **Table *2*** contains the information to determine the action type for each risk rating.

Risk Rating	**Risk**	**Actions Required**
1 - 2	Minimal	Controls Adequate
3 - 4	Low	Review controls, take actions as necessary
6 – 8	Medium	Action to be taken to reduce risk
9 - 16	High	Urgent action required. Consider halting activities / processes

Table 2 - Actions for the size

Based on these premises, the risk analysis will include the possible hazards, person's likely to be affected, existing control measures and the actions that will be taken to mitigate these risks. This information will summarize the possible risks of all the scenarios, highlighting the most critical issues and the safety measures needed to mitigate them.

The risk evaluation study played a decisive role in the selection of the safety devices and the controller, based on the requirements and the device capabilities.

3.1. Industrial robot implementation

Currently, the only robotic platform using an industrial robot is the **UC2.2 implementation in Tampere University**. Therefore, this use case will be used to describe how safety is ensured in REMODEL when working with an industrial robot. The test bed in TAU premises contains the Yaskawa SDA10F, which is a **dual armed industrial robot** with a payload of 10kg per arm, as the primary robot manipulator. And therefore, the constructed cell (containing the ELVEZ test bed) has safety implementations which comply to the guidelines and requirements of **ISO 10218:2011**.

3.1.1. Safety requirements

The employment of an industrial robot at TAU makes the safeguarding of the test bed comparatively simpler, as human operators usually do not have to get into close proximity with the moving elements of the platform. Nevertheless, some of the medium and high level risks which were taken into consideration while determining the safety devices to be used are highlighted in Table 3.

Hazard	Person's likely to be affected	Existing Control Measures	Risk rating (see Table 1)	Actions taken to mitigate risk	Residual risk rating
Exposed Robot cell	Visitors and unrelated occupants of the lab	Restricted lab access without supervision for visitors and safety training for other lab users	3 x 3 = 9	Include warning signs and safety barriers.	1 x 3 = 3
Person enters in the cell during operation	Operator	Protective gloves and safety shoes.	2 x 4 = 8	Employ door switches, light curtains and emergency stop buttons, which trigger safety errors when there is a perimeter breach	1 x 2 = 2
Person in the cell while operation starts	Operator	Protective gloves and safety shoes	3 x 4= 12	Employ door switches, light curtains and emergency stop buttons, which trigger safety errors The RESET button to clear the errors is outside the cell, forcing the operator to exit it	1 x 2 = 2

Table 3 Major Risks Identified for UC 2.2

3.1.2. Safety implementation

The layout of the safety devices employed around the various sides and access points to the robotic cell are shown in Figure 3 and Figure 4. The devices primarily used for the current implementation of the UC 2.2 are physical E. Stop buttons, Omron industrial light curtains, and Omron retro-reflective door switches (the provided hyperlinks lead to the product page). The safety PLC used is an Omron CSG320 with provisions for Digital and Analog input and outputs. The safety logic is created and exported to the PLC by using the proprietary software Sysmac studio. After the logic for the system safety is updated into the PLC, the requirement for Sysmac studio is eliminated in this implementation. See Figure 5 for the safety PLC.

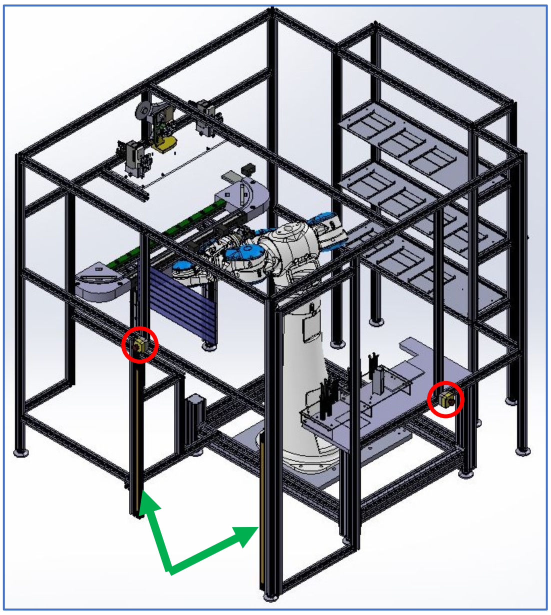

Figure 3. Cell Displaying E.stops (surrounded in red) and Light Curtain (green arrows)

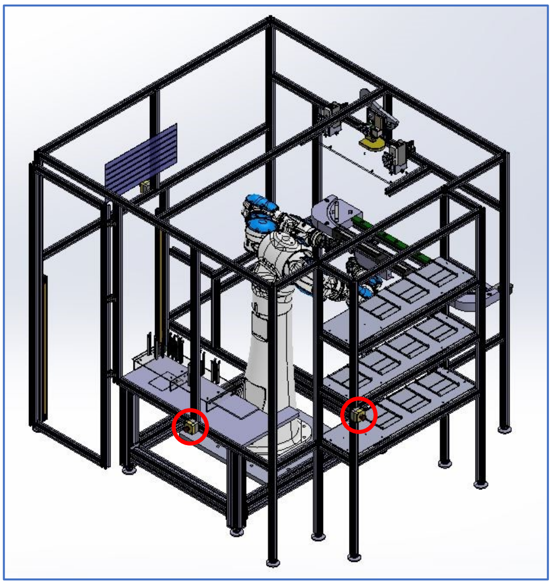

Figure 4. Cell displaying E.stops (surrounded in red) and Light curtain- Alternate view

Figure 5. Omron Safety PLC

The light curtain is primarily used to prevent any other entity except a mobile robot (unrelated to REMODEL) to enter the robotic cell. The door switches are used to prevent a human from entering the cell while the robot is online and is performing any operations. And the Emergency stops are used for stopping all activities inside the cell by an external observer, to prevent accidents or as a safety precaution while entering the cell. See Figure 6 for safety devices. There is an additional E. stop button provided in the teach pendant of the Yaskawa, and that serves as a floating failsafe which can be carried around by the programmer while performing tests. The robot is also connected to the safety PLC, wherein it could generate a signal to signify if the safety of the system has been compromised, and immediately deactivates the servo motors of the robot.

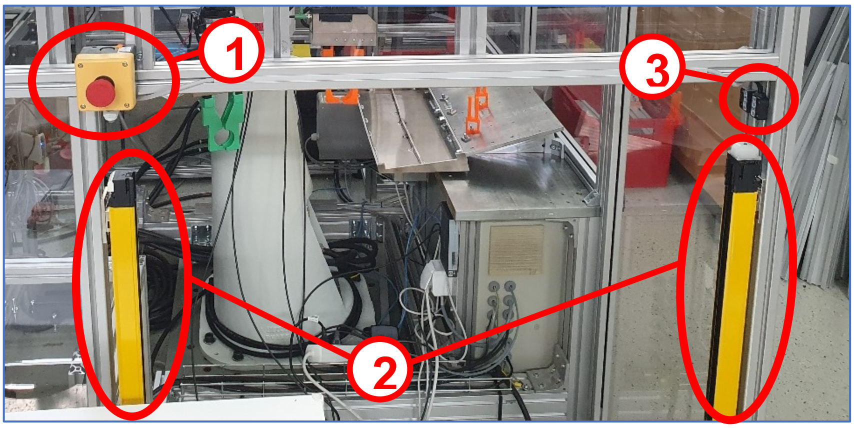

Figure 6. Safety devices: Emergency stop buttons (1), light curtains (2), and door switch (3)

Furthermore, the triggering of any of the above-mentioned safety devices, sets a flag in the safety PLC which stops all the normal functioning of the devices of the cell. The flag must be cleared before normal operations could resume. This can be performed by pushing a physical RESET button provided in the setup outside the perimeter of the test bed, at a safe distance away from moving elements of the cell. This can be seen in the safety PLC program in Figure 7, where a reset-set function block is used to determine the *cell_safety_OK* status, that is later assigned to the digital outputs of the PLC. Therefore, even if there is not any active alarm (*Ready_for_reset*), it is necessary to do a reset, with the physical button (*Reset_I*) or from ROS (*ROS_reset_PLC*). However, the reset from ROS has been disabled for this implementation, to avoid that the user can reset the system using the UI inside the cell (*ROS_reset_PLC* is always False). Additionally, if the reset button is pressed but there is still any active alarm, the *Ready_for_reset* signal will remain True and, therefore, the *cell_safety_ok* will remain False.

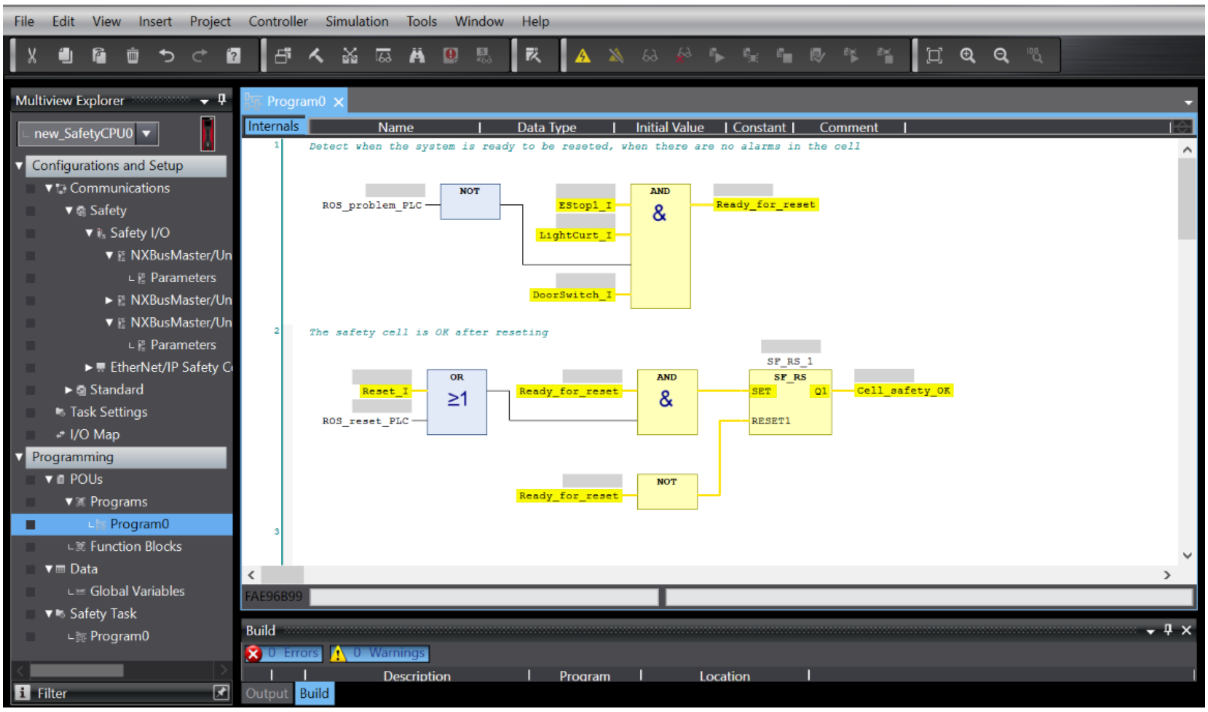

Figure 7. UC2.2 Safety PLC program

By installing this setup, we can eliminate or de-escalate the various risks which were initially identified in 3.1.1

3.1.3. Safety tests

Basic tests were initially performed to check the robustness and response of the safety devices and the safety controller, and to evaluate the reliability of the devices while performing tests with the robot. These tests included:

- Entering in the cell through the door during operation. The robotic platform stopped, and the state changed to alarm.
- Entering in the cell through the mobile robot entrance during operation. The robotic platform stopped, and the state changed to alarm.
- Pressing the emergency stop buttons during the robot operation (all of them were tested). The robotic platform stopped, and the state changed to alarm.
- Trying to start the robotic platform operation while being inside the cell. The operation didn't start, and the platform was still in alarm state.

- Trying to start the robotic platform operation after clearing the active alarms but without pressing the reset button. The operation didn't start, and the platform was still in alarm state.
- Trying to reset the alarms having still some active alarms. The alarms were not reset, and the platform was still in alarm state.

All the tests were successful, demonstrating the effectiveness of the platform's safety. During all these tests, the safety status was successfully updated in the RSM and displayed in the UI. A video compiling different safety tests can be found in https://drive.google.com/drive/folders/1_NGHp4jv_I621yKudVRyCEB0JSwcodYW?usp=sharing. The tests performed in each of these videos are described in Table 4.

Additionally, the test bed has been in use for 20 months since the current set of safety devices were finalized and implemented and there have been zero unexpected failures or accidents.

Video	Description
1	• The user starts the robot operation (safety is ok). • The user opens the door (door open alarm active and the robot stops) • The user enters inside the cell and closes the door, he tries to start the robot again, but it doesn't move (still in alarm state, door open signal inactive but not rested). • The user resets the alarms (safety is ok) and he is able to start the robot operation again.
2	• The robot is moving, and the safety is ok. • The user put his hand in the mobile robot door and it is detected by the light curtain stopping the robot. • The system moves the hand away from the light curtain area. The alarm is not active anymore, but it hasn't been reset, so the robot operation cannot be started (platform in alarm state). • The user resets the alarms (safety is ok) and he is able to start the robot operation again.
3	• The user starts the robot operation (safety is ok). • The user presses the emergency stop button and the robot stops. • The user unlocks the emergency stop button. The alarm is not active anymore, but it hasn't been reset, so the robot operation cannot be started (platform in alarm state). • The user resets the alarms (safety is ok) and he is able to start the robot operation again.

Table 4. Videos of the safety tests with the industrial robot

3.2. Collaborative robot implementation

Except UC2.2 implementation in Tampere University, all the other platforms implemented so far use collaborative robots. All these platforms have similar requirements in terms of safety, therefore just **UC2.1 implementation in TECNALIA** will be documented as an example of how safety is ensured in REMODEL when working with a collaborative robot. This testbed includes **two Kuka LBR iiwa collaborative robots**, two Schunk WSG50 electric grippers and a workbench specifically designed for wire-harness manufacturing. A fenceless robotic cell is utilized which implements a collaborative robotic cell following the guidelines and requirements of **ISO 10218:2011** and **ISO 15066:2016**.

3.2.1. Safety requirements

Hazard	Person's likely to be affected	Existing Control Measures	Risk rating (see Table 1)	Actions taken to mitigate risk	Residual risk rating
Collisions with the environment due to misuse of teleoperation devices.	Operator and programmer	Emergency button in teaching area.	3 x 3 = 9 Medium-High	Additional operator/programmer in the initial training phase to manage the emergency button. Only trained personnel can perform teaching.	2 x 2 = 4 Medium-Low
Entrapment of hand/fingers with gripper in teaching using direct interaction through gravity compensation.	Operator and programmer	Protective gloves.	3 x 2 = 6 Medium-High	Only trained personnel can perform teaching. Add handle in gripper to ensure that hands are out of reach of the fingers.	1 x 2 = 2 Low
Collision while operator provides raw materials required for assembly	Operator	Protective gloves and safety shoes . System status is Paused.	2 x 3 = 6 Medium-High	Emergency stop in workbench. Only trained personnel can enter the cell. Add signals with safety procedures.	1 x 3 = 3 Medium-Low

Collision between operator and robot during the manual assembly of the wire harness.	Operator	Protective gloves and safety shoes . System status is stoped.	2 x 3 = 6 Medium-High	Emergency button pushed during the manual assembly process. Only trained personnel can enter the cell. Add signals with safety procedures.	1 x 3 = 3 Medium-Low
Person enters in the cell during operation	Operator	Protective gloves and safety shoes. Emergency stop in workbench.	2 x 4 = 8 Medium-High	Safety devices detecting persons entering the cell and stopping the manipulator. Signs and safety procedure around the cell. Only trained personnel allowed to enter during operation.	1 x 4 = 4 Medium-Low

Table 5 Major Risks Identified for UC 2.1

3.2.2. Safety implementation

The central elements of the robotic cell are two Kuka LBR iiwa robots placed around the perforated workbench that is used for the assembly of the wiring harnesses. The main idea on the implementation is to define a virtual fence around the workbench and robots using safety laser scanners, as shown in Figure 8.

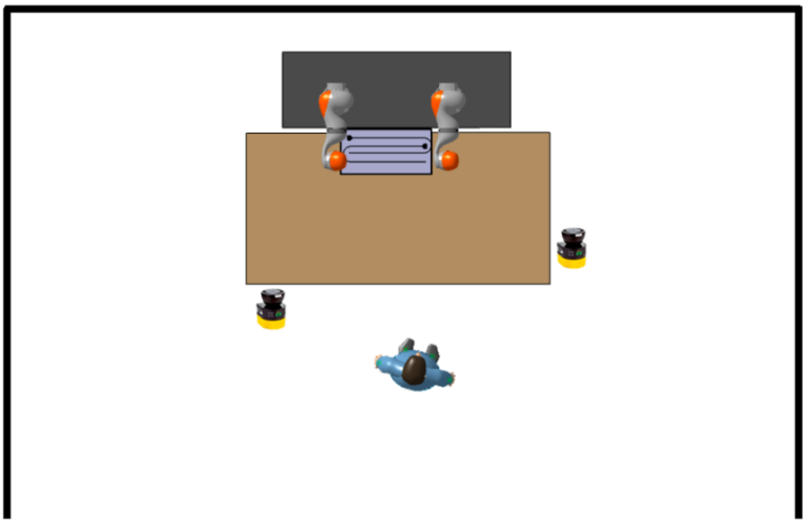

Figure 8 - UC2.1 cell with Sick microScan3 laser scanners

The main elements of the collaborative safety implementation are listed below:

- **Sick FLEXI soft safety PLC** that will gather all safety signals and merge the information.
- Two **Sick microScan3** safety laser scanners.
- **Three colour signal lamp** to indicate the safety status.
- Additional **emergency button** to be placed around the cell to complement the laser-based safety.

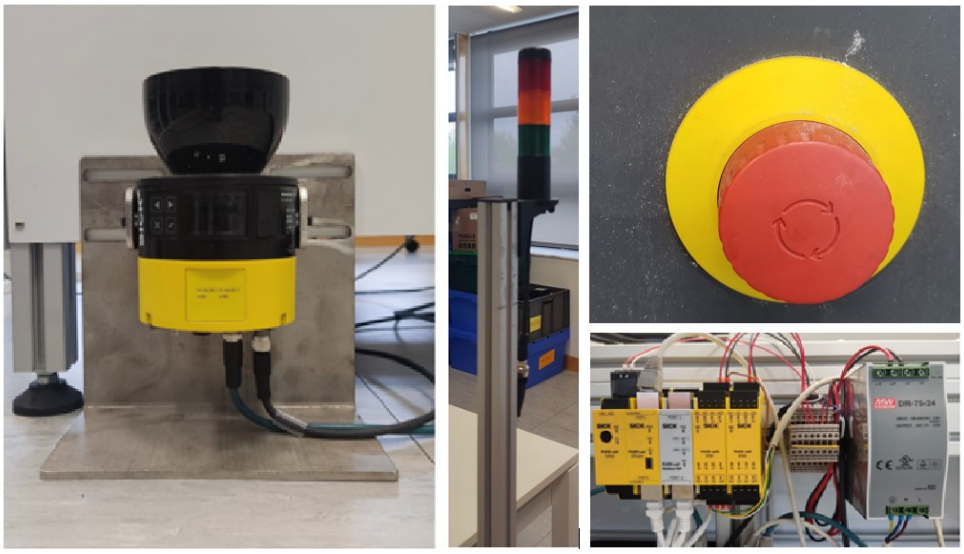

Figure 9 - Safety devices included in UC2.1

Initially, one main consideration has been taken into account regarding the laser scanner placement. As the production areas constantly change due to modifications in the production line, it is necessary to allow an easy and simple change in the scanners’ placement. Therefore, it has been decided to mount the Sick microScan3 scanners in metal brackets to facilitate its placement in different positions of the cell.

Figure 10 - Sick microScan3 scanners on the metal brackets

Once placed the laser scanners, two different areas have been defined in the robotic cell (Figure 11):

- **Emergency stop area:** Red area near the Kuka LBR iiwa arms where an emergency stop signal is activated whenever a space violation is detected. This area defines a virtual safety fence around the robots.
- **Warning area:** Yellow area surrounding the *emergency stop area*. In the actual implementation, any violation of the area only triggers a visual signal although future developments could include a speed reduction on the robots.

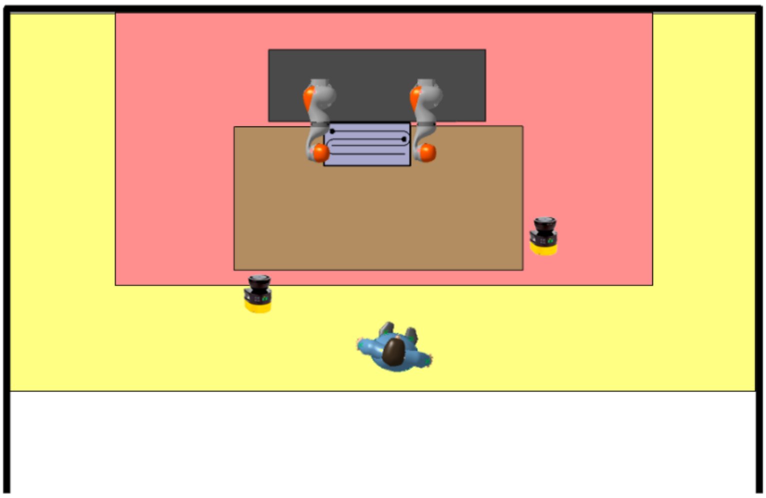

Figure 11 - Safety areas of the UC2.1 robotic cell

Based on these warning and emergency stop areas, both laser scanners have been programmed using Sick Safety Designer software (Figure 12) in order to include these regions on the scanners and trigger the safe digital output signals of the microScan3 scanners.

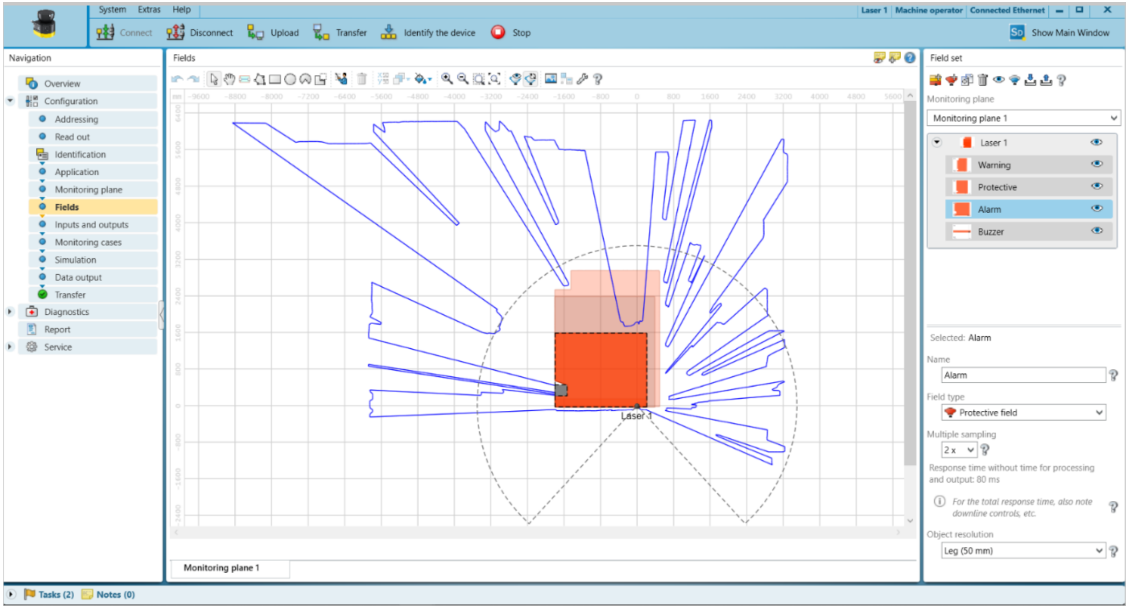

Figure 12 - Safety area definition in Safety Designer

To merge the different signals (laser scanners and external emergency stop), a program has been implemented on the Sick FLEXI soft safety PLC using also the Safety Designer software (Figure 13).

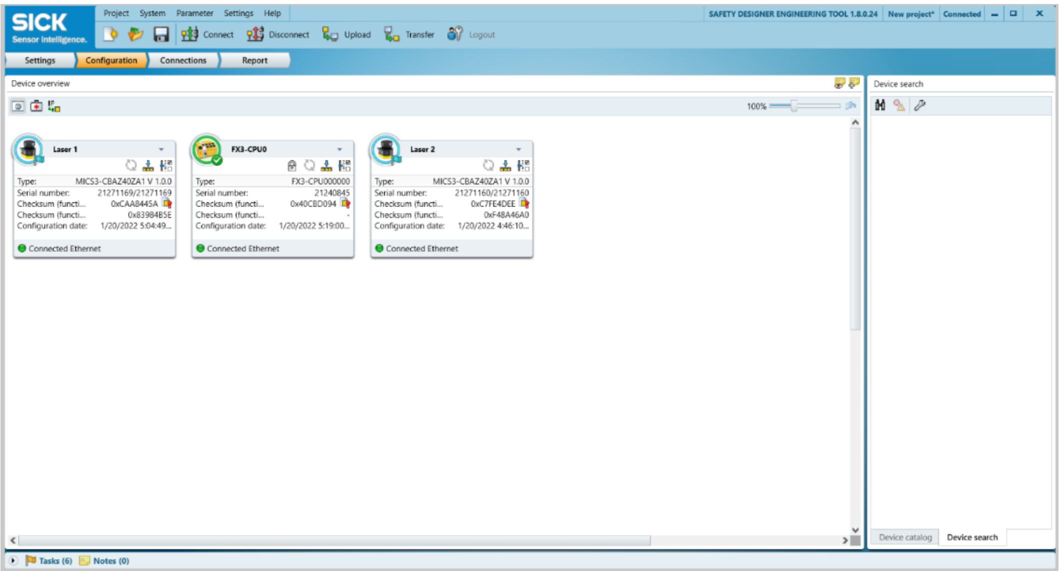

Figure 13 - Integrating Sick microScan3 scanners in safety PLC

This program merges all received digital signals and activates the required signals defining the safety status of the cell:

- **Emergency stop:** This state is activated whenever a laser scanners detects a violation of the emergency area or the remote emergency stop is pushed.

- **Warning state:** This state is activated whenever a laser scanner detects a violation of the warning area.
- **Safe state:** This state indicates that the system is safe as there is not any violation of the robot area.

The developed PLC program is shown in Figure 14.

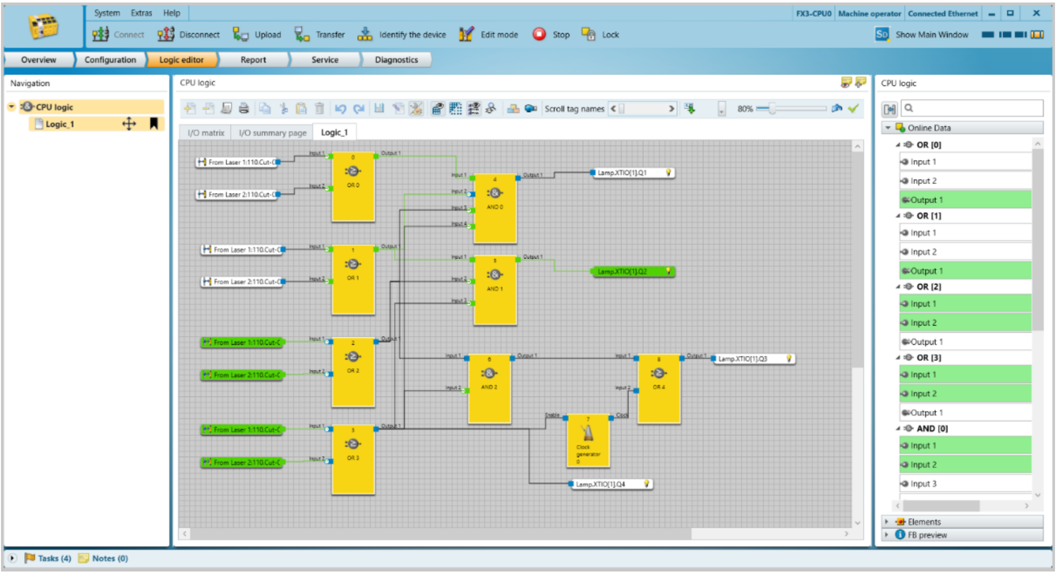

Figure 14 - Safety program developed in Safety Designer

Finally, a three colour signal lamp has been used to indicate visually the safety status and assist operators on the identification of unsafe situations. The signal lamp provides feedback of the previously exposed safety states:

- **Emergency stop:** Red light active and auditive signal triggered.
- **Warning state:** Yellow light active.
- **Safe state:** Green light active.

With this implementation, a safe fenceless environment has been achieved. Additionally, whenever the environment or the placement of the laser scanners change, it will be required to reconfigure the safety areas of the Sick microScan3 scanners, without any modification of the PLC program.

3.2.3. Safety tests

Basic tests were initially performed to check the robustness and response of the safety implementation while performing developments and tests with the robots. These tests included:

- Approaching the workbench during the execution of tasks. The robotic platform stopped, and the safety state changed to emergency stop.
- Pressing the emergency stop button during the robot operation. The robotic platform stopped, and the state changed to emergency stop.

- Trying to start the Kuka LBR iiwa robots while being inside the emergency stop area. The robots could not be set in *run* mode and the platform was still in emergency stop state.

All the tests were successful, demonstrating the effectiveness of the platform's safety. A video showing how the laser scanners and the safety areas work can be found in https://drive.google.com/drive/folders/1_NGHp4jv_l621yKudVRyCEB0JSwcodYW?usp=sharing. In this video, it can be seen how the lamp color changes to orange when the operator enters in the warning area, and to red when he enters in the emergency stop area. Additionally, when the operator is in the emergency stop area, it can be heard that an alarm turns on.

4. Conclusion

This deliverable documents the implementation of the REMODEL Safety Manager (RSM) at the TRL 5 level, and it demonstrates how the developed solutions can be very easily implemented at TRL6 with minor updates (complying to the safety requirements and standards of the industry and it's governing bodies). The highlights of the deliverable include the implementation of the RSM in two specific usage scenarios i.e., an industrial robot and a cobot application. The industrial robot is enclosed in the cell and any external intrusion during the execution of the task triggers the safety devices (light curtains and door switch) and the pushing of the E.stop button, causes all the activities of the operation performed by the manipulator to shut down. This is the status until all the error situations are cleared; the personnel are at a safe distance from the cell; and the RESET button is pushed. The robotic platform is now ready to continue its operation. The cobot setup is similar to an extent (the physical cell is replaced by a virtual fence) and utilizes laser scanners to create variable speed zones and E.stops. When the personnel approaches setup there are various visual and auditory warnings and indicators, to make them aware of the operation taking place.

The implemented RSM can additionally visualize the system safety status on the UI. The use of ROS in setting up the communication platform between the safety devices and the user's workstation are for representing the system's safety state (which can be utilized by other modules of the REMODEL system). The actual safety implemented runs on a higher priority protocol of the safety controller, so the system's security is never compromised due to delay in device communication.

Therefore, the implemented safety solutions and the RSM greatly reduces the risks estimated during the early stages of the project, while making provisions for active integration into the rest of the developed modules for the project REMODEL, by utilizing ROS.