**Risk Assessment**

**Validation**

**Contents**

[Foreword 2](#_Toc498682614)

[Limits of the robot system 3](#_Toc498682615)

[Hazard identification 17](#_Toc498682616)

[Risk Estimation and Evaluation 18](#_Toc498682617)

## Foreword

The present analysis is intended for research purpose only. The research topic aims at developing a semi-automated tool for risk assessment, based on formal model representation of the human-robot application under evaluation, followed by a model checking in charge of identifying hazards and estimating risks.

The manual risk assessment in intended for the purpose of validation of the automatic tool, i.e. its ability to replicate to some extent the expert-level risk assessment.

For the purpose of balancing the boundary conditions of the manual vs. automated risk analysis, the description of the application (intended use) is provided in a draft version: this level of description corresponds to an initial round of analysis of the application with the end user. One additional round of clarifications, further details and structured analysis of workflows or activities can be done. The level of description is balanced with respect to the starting point of formalization by the automatic tool under investigation.

The application under analysis is set to a high level of interaction between humans and robot, due to:

* Close proximity inside a shared workspace, with tasks to be performed on the same location and/or at the same time;
* A high degree of variability in composing the task workflows due the degrees of freedom in assigning roles and execution modes by either operators or the production planner;
* Loose requirements in terms of timing and synchronization: main robot tasks are not time-critical, can be highly parallelized with respect to human tasks, time-windows for both manual activities and robot activities are substantially larger than the minimum nominal task execution time.

This set of conditions is derived from Flexible Manufacturing Systems technology and is under development/deployment in a machine-tool end user shopfloor (SME, North Italy). The main application purpose is to

* Release operators from single-oriented, station-bound activities towards multi-machine supervision
* Provide larger flexibility in the management of manual tasks and workspace usage

Performers of the present risk assessment are not liable for any intentional or unintentional omission or fault.

The following remarks and/or exceptions apply to the current analysis with respect to the full procedure (ISO 12100).

* Start up and commissioning phases are not considered.
* Limits of machinery related to other sources of power than electrical are neglected or not used (e.g. hydraulic power for automatic clamping fixtures). No hazards related to power sources need to be reported.
* Only mechanical hazards should be considered (impacts, crushing, entanglement, etc) because of the focus of the analysis on physical human-robot interaction. No noise, vibration, electrical shock, etc are considered as hazard sources.

## Limits of the robot system

***Filed according to ISO 12100 §5.3.2 and EN ISO 10218-2 §4.3.2a***.

The robot system is dedicated to a number of assistive tasks in material handling, inspection and assembly of pallets for Flexible Manufacturing Systems (FMS).

Production environment and objectives

|  |  |
| --- | --- |
| The property of a FMS is the ability to schedule a variable product mix in real time depending on some production optimization. Parts are machined and transported inside the FMS. Parts to be machined are loaded/unloaded on/from pallets (see Figure 1). Entry/exit stations for parts are Load/Unload Stations (LUS) dedicated to assembly and testing (see Figure 2). LUSes are the only stations with direct access for operators in the whole FMS  The production mix – and the availability of specific pallets at LUSes – is scheduled by the FMS. Parts/pallets can be called/assigned to LUS at any time, carrying any type of parts.  Objectives in adopting a collaborative solutions (parts of specifications):   * Relieve Operators from heavy duty manual tasks, including but not limiting to loading/handling, screwing/fixing fixtures, etc * Allow Operators supervisory tasks over multiple LUSes, i.e. detach operators from a single station also along the same task * Increase the traceability of operations (logged by the robot system) and reduce errors in pallet assembly | Figure 1 – pallet inside a LUS (open doors) |

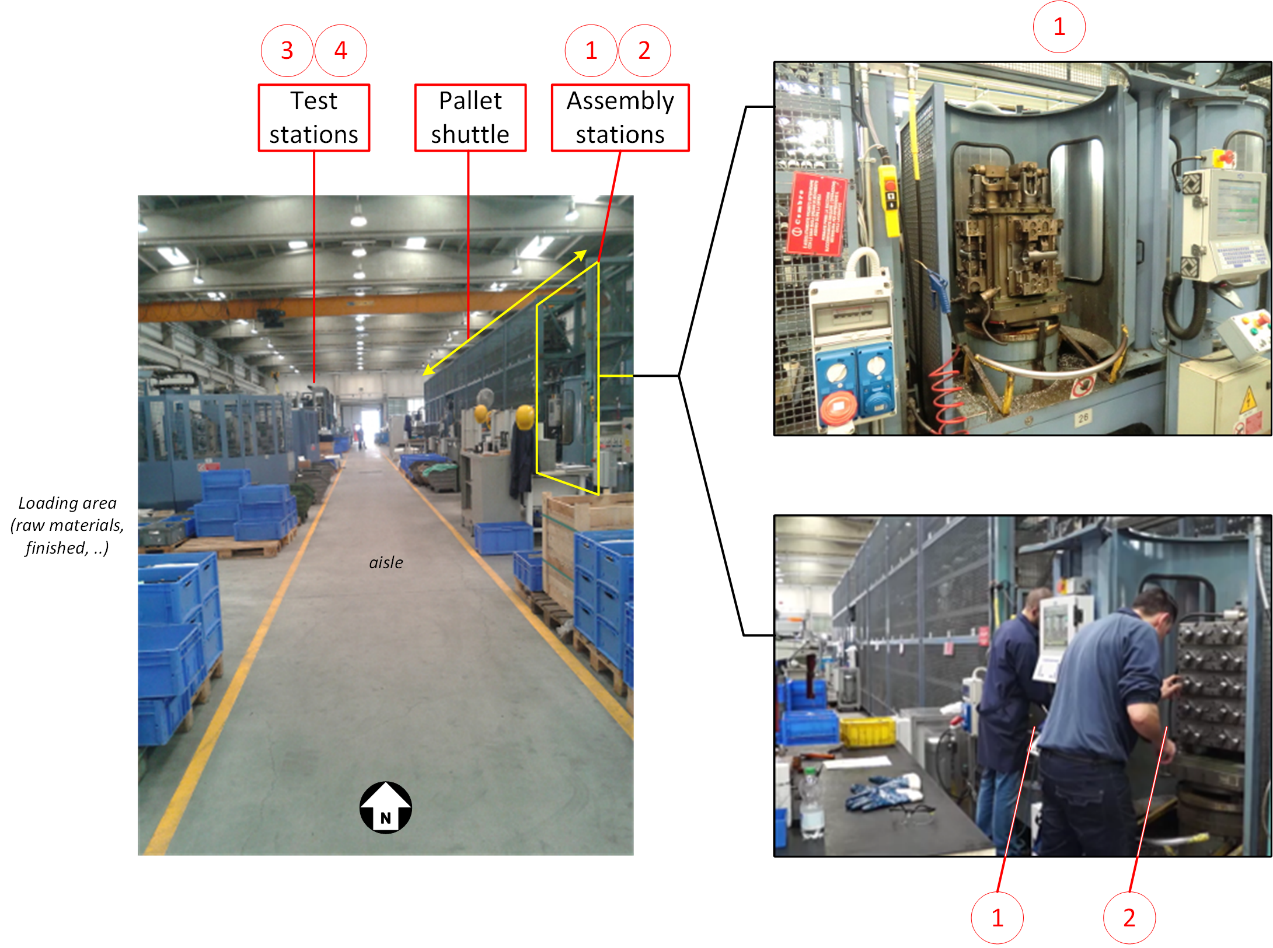


Figure 2 – overview of the shopfloor hosting the FMS

Layout and overview of operations

One single robot platform (mobile unit + manipulator) is used in a restricted area (see Figure 3) of the FMS shopfloor in Figure 2.

The robot unit (R) can

* relocate in correspondence of stations 1, 2 and 3, in predefined positions (depicted in Figure 3),
* be relocated by operators slightly around their predefined positions, within the reaching of stations 1,2 and 3 (+/- 200 mm),
* travel in the whole workspace (blue area in Figure 3),
* access the loading area.

According to North-bound convention in Figure 3, more frequent routes for R are along W-E direction.

Two (2) operators (OP1 and OP2) are allowed to perform task in the area. Other operators may access the area without intended task to perform (e.g. cross from/to adjacent shopfloor areas).

According to North-bound convention in Figure 3, more frequent routes for OP1 and OP2 are along W-E direction. More likely routes for crossing operators are along N-S direction.

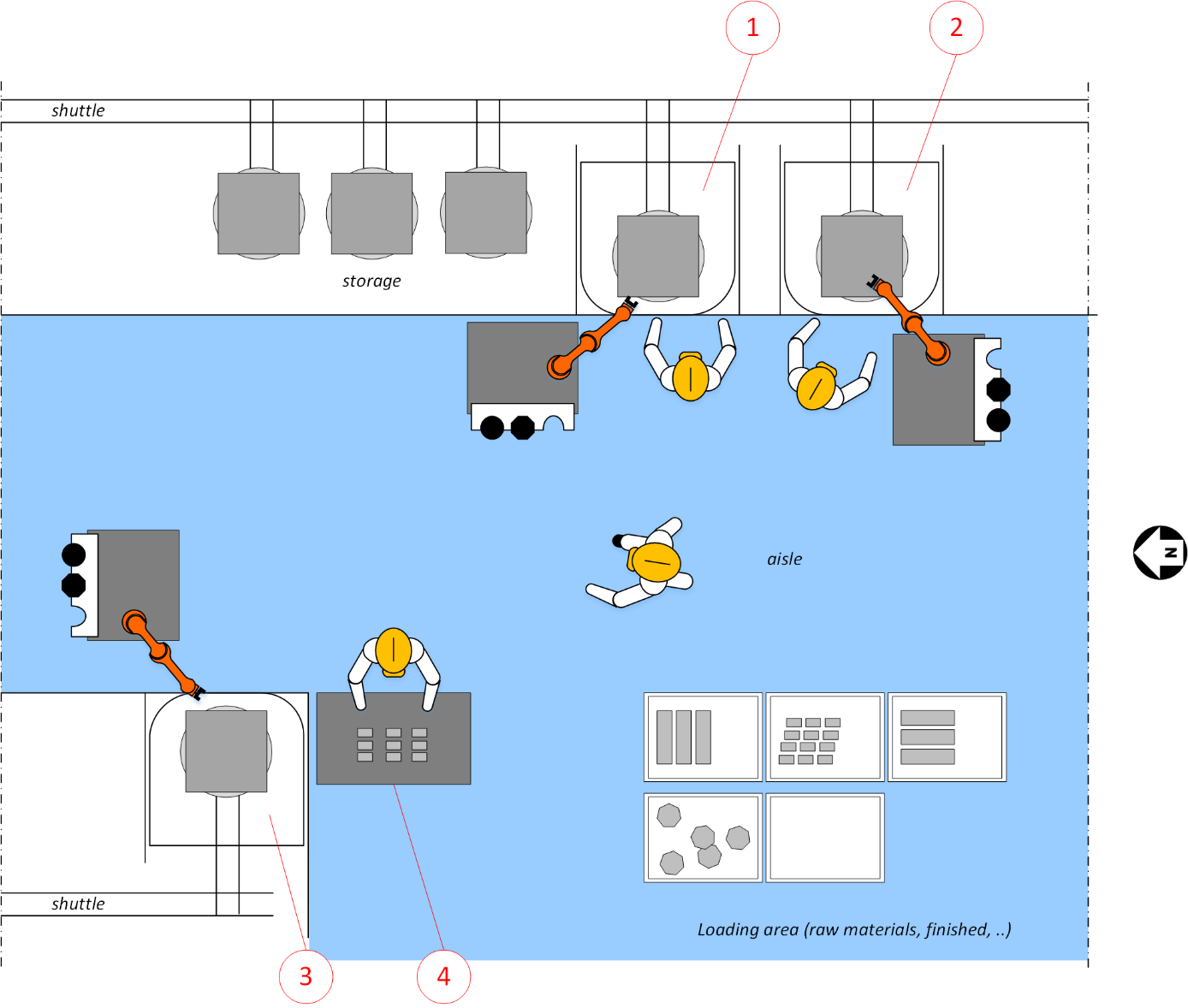


Figure 3 – layout (top view, unsized). Robot and operator are depicted (duplicated) in working locations (1 robot and 2 operators are intended for operations)

**Use Limits (EN ISO 10218-2 4.3.2a)**

|  |
| --- |
| **Intended use** |
| The robot system is intended to provide assistance for the manipulation of workpieces in machine tool Load/Unload Stations (LUS) 1, 2 and 3 (see Figure 3), namely including the following operations:   * Assembly/disassembly of raw material and/or finished parts on pallet fixtures * Inspection and measurement of pre/post-machining parts and fixturing * Handling of parts from/into boxes   In ALL operations some degree of collaboration is allowed, i.e. Operators can intervene, modify or replace robot tasks.   |  | | --- | | **IMPORTANT NOTE**: structure of the intended use section.  The main robot-assisted intended tasks are:   * Pallet assembly at stations 1 and 2, including bin-picking * Pallet disassembly (reversal of assembly) at stations 1 and 2, including bin-dumping * Pallet inspection at station 3 * Lead-through programming of assembly/disassembly/inspection tasks (trajectories, parameters, etc) at stations 1, 2 and 3 * Material loading (receive boxes on top of platform)   Other manual tasks include:   * Manual loading of parts/boxes (on top of robot unit) * (additional) visual inspection of pallet at stations 1, 2 and 3 * Manual assembly/disassembly of pallet at stations 1 and 2 * Manual measurements of parts at station 4 * Cleaning pallets at stations 1 and 2 * Kitting tools and parts at stations 1,2 and 3 * General supervision (programming other tasks at HMI during operations, consulting production data at HMI, ..) at stations 1, 2 and 3   **ALL** combinations of robot/manual tasks are admitted, e.g. robot holding, operator screwing jigs. Program combinations are assigned at programming/setup time (first run of a production batch).  **ALL** resulting workflow variants can be halted and later resumed, OR changed into another variant, e.g. quitting a manual task and assign the robot to proceed autonomously.  In the following paragraphs, details about single tasks and example variants are provided.  At the end of the section, a general task outlook and list of example variants is provided.  For the purpose of the risk analysis, all reasonably foreseeable situations need to be considered. |   Detailed operations – hybrid (collaborative or autonomous) assembly/disassembly   * Parts: 2 part types are considered [[1]](#footnote-1)   + **PTA**: a 3 steps part, aluminium, 3 kg, size 300x60x35 mm (PTA\_RAW), assembled on fixtures in 2 intermediate steps (see Figure 4).   PTA machining cycle is completed in 2 rounds:  (disassembly and exit) PTA\_P2 removed from PTA\_BP2  (disassembly and assembly) PTA\_P1 from PTA\_BP1 into PTA\_BP2  (enter and assembly) PTA\_RAW in PTA\_BP1    Figure 4 – item PTA, with machining steps (left) and fixture on pallet (right)   * + **PTB/PTC**: a pair of 3 steps parts, steel, 0.050 kg, size 60x20x10 mm (PTB/C\_RAW), assembled on fixtures in 2 intermediate steps (see Figure 5).   Each single item is assembled for both steps in a 3x4 matrix of jigs, half housing PTB, half housing PTC. Each jig has 2 mounting location (1 for each machining step)  PTB/PTC machining cycle is completed in 2 rounds:  (disassembly and exit) PTB\_P2 removed from PTB\_BP1…6, top seat  (disassembly and assembly) PTB\_P1 from PTB\_BP1…6, bottom seat, into PTB\_BP1…6, top seat  (enter and assembly) PTB\_RAW in PTB\_BP1…6, bottom seat  (PTC correspondingly in jigs PTC\_BP7…12)    Figure 5 – item PTB/PTC pair, with machining steps (left) and fixture on pallet (right)   * Location and tasks: the assembly/disassembly operations are done at any LUS, according to labelling conventions in Figure 6  |  |  | | --- | --- | |  |  |   Figure 6 – notation of working locations for PTA/PTB/PTC assembly/disassembly and testing on LUSes  Additional notable locations (Figure 6):   * + PTx\_HBP: local homing, in front of pallet to be programmed for starting approach/depart movements, resting on holding trajectoryies, returning in case of failure, etc;   + BP: box location, on robot unit trolley, where boxes can be placed for local bin-picking or returning of finished parts; Operator can access any box;   + B: buffer location on top of robot unit for preparing PTx\_RAW picked from BP, before loading into PTx\_BPx. Useful for limiting the number of tool changes (recall 1 tool for bin picking, 1 tool for handling)   + TC1…3: tool change seats of robot tools. Tools (see below) are stored on the top-side edge of the robot mobile platform.  |  | | --- | | NOTE: a prototype version for the purpose of visualization of components is depicted in Figure 7:    Figure 7 – prototype version (bot fixtures mounted on the same pallet, no LUS station, unfinished layout) |  * Workflow of assembly (example): the assembly subtask is described in form of Activity Diagram in Figure 8 and Figure 9 for PTA and PTB/PTC, respectively.   + One of the possible variants for the part assembly is represented: robot handling parts and placing into jigs, operator fixing the jigs. The mirror variant is also possible (operator picking and placing parts, robot tightening the jigs).   + The main execution path (red lines in figures) is completed with some deviations upon conditional execution (i.e. presence of failures, unexpected conditions of the pallet, etc)   + In case of collaborative mode abort, any autonomous mode shall require the robot to take over the operator actions (i.e. screwing in Figure 8): in such cases, the nominal workflow is altered according to the following considerations:     - actions for changing tools shall be included. In the execution mode of Figure 8, screw/unscrew require the robot to move to TCx, change the tool and return to assembly/disassembly location   OR  screwing can be postponed to all placements so as to limit the number of tool changes (all unscrewings, all handlings, all fixings);   * + - conditional execution based on human decisions makes the workflow to be suspended until an explicit resume by the operator. In this case, the execution is paused and the operator notified (by HMI)     Figure 8 – example workflow for PTA assembly/disassembly    Figure 9 – example workflow for PTB/PTC assembly/disassembly  Detailed operations – hybrid (collaborative or autonomous) testing   * Parts: same pallets (PTA and PTB/PTC) are inspected with camera in station 3 * Location of operator: occasional (e.g. troubleshooting) presence. If present, poses as in Figure 6 * Workflow: the robot starts at home position, then moves and stops in stored recording poses for taking measures with the sensor. Sequence of poses is programmed in setup phase with lead-through programming modes. Trajectories among recording poses are programmed in setup phase.   Detailed operations – lead-through programming (teaching)  On first part loading (e.g. first job in each PTA/PTB batch), the FMS alerts the robot unit and the operator (through HMI) that new poses and parameters need to be recorded for the specific job.  Such setup phase include:   * Task configuration on the HMI  |  |  | | --- | --- | | * selection of the number of slots (i.e. jigs) available on the pallet (e.g. 2 for PTA, 24 for PTB/PTC); * selection of jig topology in matrix form (e.g. 2x1 for PTA, 3x4 for PTB/PTC * speed tuning * confirmation/update of template manipulation routine with additional sub-actions: e.g. the template routine is   1. approach to jig   2. move into part seat   3. press into the fixture   4. open fingers   5. depart from pallet to home   6. [repeat for all jigs]   While a jig need to be turned upside-down before inserting: an additional move and grasp need to be inserted between steps 4 and 5.   * Selection of assigned tool(s) | Figure 10 – portable HMI for task selection and configuration |  * Hand-guiding teaching of template home PTA/PTB\_HBP * Hand-guiding teaching of paths (approach and depart) from home PTA/PTB\_HBP to PTA/PTB\_BP poses (see Figure 11) * Verification of the resulting trajectories     Figure 11 – user teaching poses on PTB/PTC pallet (prototype version)  **Manual operations**.   * In pallet assembly/disassembly (regular operation repeated for all batches), manual operations might include   + bolt tightening/loosening with tools (wrenches),   + inserting/removing parts (by hand),   + manipulating jigs (by hand),   + picking/returning parts from/to boxes   + clean fixtures      * In pallet inspection, manual operations might include   + visual inspection of pallet (no contact)   + assembly check (by touching parts and jigs)   + measurement of parts while in fixtures with tools (gauges) * in teaching, manual operations might include   + hand-guiding the end effector in to-be-recorded locations (lead-through programming)   + interaction with HMI for programming (recording, holding/resuming/quitting motion) * in loading/unloading boxes, manual operations might include   + loading empty/full boxes onto the mobile unit top surface   + unloading the robot unit   **Setup, start up and verification.**  NOT CONSIDERED: commissioning and startup of the application is not part of the present risk analysis (see Foreword).  **exclusions**:   * OP1 and OP2 are operators normally assigned to pallet assembly tasks, and trained in the use of the robot unit. No other operators are cleared for the usage of the robot system * No other AGV of manned lift are allowed to access the restricted area during robot operations. In this case a dedicated procedure is initiated. * No suspended loads are present during robot operations. In case of transport of suspended load, a dedicated procedure is initiated.   Overall workflow  Due to the runtime assignment of parts to either station 1 or 2 by the Manufacturing Execution System (MES), operators OP1 and OP2 can freely decide how to perform assigned tasks. See example assembly workflows in Figure 8and Figure 9, where a default/frequent choice is highlighted. In Figure 9 (PTB/C assembly), for instance, long part placement sequences by the robot could let OP1 to move to different stations and resuming later.  The default configuration is with OP1 supervising stations 1 and 2, and OP2 supervising station 3 and working on station 4. OP2 is expected to frequently move in station 1/2 upon request/need.  Robot unit is mostly dedicated to stations 1 and 2, moving between the two upon OP1 decision. Assignment of robot unit to tasks/stations is decided at start up of every new job (once per day with 2 parts PTA/PTB in the production plan). Task assignment of the robot unit can be altered during operations, most frequently switching to autonomous task execution while (mostly) OP1 is released form the same collaborative task.  Robot unit can be frequently assigned to move and fetch/dump materials into the load/unload area. During robot load/unload, OP2 is frequently required to cooperate with the robot unit while OP1 is less frequently required to cooperate with the robot unit.  As a result, OP1 is expected to mostly stay in station 1 and 2 area, occasionally moving to load/unload area, while OP2 is expected to move in all locations.  In the following, a typical storyboard is provided with most frequent options. Keywords “meanwhile” and “options” are intended to describe the most likely situations that can fork from any previous execution status.   1. OP2 manually measures finished parts in station 4   *MEANWHILE*   1. MES loads the next job (PTA, assigned to station 1) 2. OP1 and R move to station 1 3. OP1 teaches the robot poses, and start configuring the subtasks   *OPTIONS*   * OP1 fixes jigs, while R handles parts (bin-picking, placing on fixture, holding if necessary) * OP1 handles parts, R fixes jigs. * OP1 handles parts, R paused. When OP1 finished, R fixes all jigs * OP1 move to station 2, R runs the entire routine autonomously  1. MES loads the following job (PTA again on station 2) 2. OP1 repeats with available options 3. MES loads the following job (PTB on station 1) 4. OP2 is asked to join station 1, while OP1 is active on station 2 5. OP2 and R at station 1, OP2 teaches poses and configures the sub tasks 6. OP2 continues working on stations 1 on PTB with available options 7. OP2 finishes the task on station 1, send the robot to station 3 for inspection 8. OP2 then move to fetch a box on loading area and carries to the robot on station 3 (ready for next load) 9. R moves back to station 1, and starts the routine autonomously 10. OP1 finishes/quits tasks on station 2 and moves in station 1 for solving jammed fixtures   *MEANWHILE, OPTIONAL/ASYNCHRONOUS task*   1. OP2 moves into loading area, calls for R, then load 1 box on the robot unit 2. OP2 joins OP1 in stations 1 or 2 3. OP1 moves to station 3 for occasional inspection 4. OP2 visits stations 1 and 2 for cleaning, while OP1 and R are active on either stations 1/2 or 3 |
| **Description of components** |
| |  |  |  |  | | --- | --- | --- | --- | |  | | | KUKA iiwa R820, with   * Gripper Schunk Co-Act WSG, electrical power, programmable   (naked version in this picture)   * Camera (flange mounted in this picture) | |  | Schunk Tool Changer WSK-015  Disassembled parts of payload side in the picture. From top:   * Automatic toolchange * Grooved flange, to inserted in concave hubs of tool buffer * Bundle of toolchange and flange, resting on one seat in the hub | | | |  | | Gripper Schunk Co-Act PGN, pneumatic power, adapted with regulated air pressure.  Rubber cover around the gripper. | | |  | | Vacuum cup for bin-picking (mounted on a UR10 robot) | | |
| **Risk-reduction measures associated to partly-completed machines** |
| KUKA R800 s/n xxx, Safety Configuration package, including range limits and power-limitation functions. Measures are of control-based safety functions (SRP/CS according to ISO 13849-1), delivered in compliance with EN ISO 10218-1:2011 §5.4.2.  Atomic Monitoring Function (AMF) as reported in Section 13 of KUKA Sunrise.OS 1.3 (Version: V1, Issued: 15.10.2014). Used functions   |  |  |  | | --- | --- | --- | | **AMF** | **Referece to Sunrise OS** | **Description** | | TCP cartesian speed monitoring | 13.8.11.3 | max cartesian speed TCP | | TCP force monitoring | 13.8.8.2 | max forza al TCP | | Cartesian workspace monitoring | 13.8.9.1 | max workspace | | Max orientation | |
| **Other energy sources** |
| * Pneumatic |

**Definition of workspaces (EN ISO 10218-2 §4.3.2b)**

|  |
| --- |
| **Definition of working areas** |
| Figure 12 – layout grid and sizes |
| **Definition of safeguarded space (ISO 10218-2 §5.10) and collaborative space (ISO 10218-2 §5.11)** |
| All robot system workspace – including the reach of tools, pallet area and bin-picking area - is defined as collaborative space.  NOTE: Being composed of a mobile unit, the robot system workspace is defined as the area in blue in Figure 12.  No guards are set in place during robot regular operations. |
| **Working areas for manual operations and other interventions** |
| The collaborative workspace is accessible by operators from all directions, if available.  Assembly/disassembly and testing of workpieces and jigs on pallets are done from the front side of pallet at stations 1, 2 and 3. |

## Hazard identification

***Filed according to EN ISO/TR 14121-2:2012, EN ISO 10218-2 §4.3 and Annex A,*** ***ISO/TS 15066:2016 §4.3***.

**Table 1 – hazards in reasonably foreseeable misuse**

|  |  |  |
| --- | --- | --- |
| **event/situation** | **Motivations for misuse** | **hazard** |
| *[very short description of the unintended situation]* | *[very short description of the foreseeability]* | *[very short description of the hazard]* |
|  |  |  |
|  |  |  |
|  |  |  |

**Table 2 – hazards in intended use**

|  |  |
| --- | --- |
| **Hazards** | **Identification (event / situation)** |
| Mechanical hazards | |
| *[very short description of the hazard]* | *[very short description of the situation deriving from intended use]* |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| Electrical hazards | |
| […] | NOT CONSIDERED |
| Thermal hazards | |
| […] | NOT CONSIDERED |
| Noise hazards | |
| […] | NOT CONSIDERED |
| other hazards | |
| […] |  |

## Risk Estimation and Evaluation

**Mechanical hazards: transient impacts**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | *[identifier]* | | | | | | | | |
|  |  | | | | | | | | |
| UNI EN ISO/TR 14121:2012-2 Tab. A.19 | ***Hazard*** | *[very short description of the hazard]* | | | | | | | |
| **Lifecycle**  *[indicate with X]* |  | Setup |  | Test |  | Normal use | | |
| [X] | maintenance |  | decomissioning |  |  | | |
| **where** | *[region of the layout, grid coordinates, labelled location, …]* | | | | | | | |
| **personnel** | [X] | developer |  | User | | |  |  |
| **Operation** | *[reference to step identifier of a workflow; reference of an action list; …]* | | | | | | | |
| ***Situation/condition*** | *[OPTIONAL - very short description of the situation]* | | | | | | | |
| ***Event*** | *[very short description of the potential harm]* | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | misuse? | Se | Cl | Notes about estimation | Initial Evaluation | Risk reduction | Se | Cl | Final Evaluation | Residual risk | Complementary measures |
| *N* | *[indicate X]* | *N* | *N* | *[indicate motivations about scores, individual scores for occurrence (frequency, probability, avoidability) or any other method]* | *[negligible, low, mid, high]* | *[indicate risk reduction strategy, e.g. safeguarding, collaborative PFL, collaborative SSM, use of sensors/equipment, safety functions]* | *N* | *N* | *[negligible, low, mid, high]* | *[OPTIONAL]* | *[OPTIONAL]* |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

1. Simplified assumption for the purpose of the present analysis [↑](#footnote-ref-1)