I-RIM Conference 2019
October 18 - 20, Rome, Italy
ISBN: 9788894580501
DOI: 10.5281/zenodo.4794414

Formal Verification-based Risk Assessment for Industrial Human-Robot Collaboration

1st Mehrnoosh Askarpour
DEIB, Politecnico di Milano
Politecnico di Milano
Milan, Italy
mehrnoosh.askarpour@polimi.it

2nd Dino Mandrioli
DEIB, Politecnico di Milano
Politecnico di Milano
Milan, Italy
dino.mandrioli@polimi.it

3rd Matteo Rossi
DEIB, Politecnico di Milano
Politecnico di Milano
Milan, Italy
matteo.rossi@polimi.it

4th Federico Vicentini
STIIMA
National Research Council of Italy
Milan, Italy
federico.Vicentini@stiima.cnr.it

Human-robot collaboration (HRC) imposes potential frequent physical interaction and/or close proximity between the two agents. Most likely, and specifically for unstructured environments, changing layouts and dynamic task allocation, the prediction of hazardous conditions may be difficult or incomplete. Nonetheless, conducting a thorough risk assessment on the mechanical hazards—physical harms to the human operator caused by the robot—is essential for collaborative systems, to define preventive or responsive mitigation mechanisms within the system. In previous works [1], [2], we have defined a methodology, SAFER-HRC, that applies formal verification for hazard identification and risk analysis of contact hazards. SAFER-HRC creates formal models of HRC applications via the TRIO temporal logic [3] and uses an automated verification tool, called Zot [4], to exhaustively search their state space for hazardous situations.

Given a UML model of the application based on a specific profile notation [5], SAFER-HRC translates it to a logic model containing: (i) logic formulae that describe a discrete representation of operator, robot and the layout, the most important entities of collaborative systems, and the executing job; (ii) formulae modeling the significant hazardous situations as described in ISO 10218-2 and ISO/TS 15066; (iii) formulae modeling human error phenotypes [6]; (iv) a formal replication of the ISO/TR 14121-2 risk estimation procedure; (v) formulae describing risk reduction measures (RRM) for collaborative modes as described in ISO/TS 15066.

SAFER-HRC does not replace human risk assessors, but it provides an automated assistant that helps them detect hazardous situations and compute the overall risk of the system. Figure 1 shows a walk-through of SAFER-HRC where, starting from UML diagrams, a formal model is automatically generated and verified. In case the model requires additional RRMs, manual intervention is needed by the human assessor to choose the best-suited RRMs for each situation.

Empirical Evaluation and Validation

SAFER-HRC is evaluated by applying it to a complex collaborative task and a large environment which is modeled in three dimensions (i.e., each discrete location has lower and upper areas, where height of areas is determined by sizes of human body). The results produced through the formal verification tool are then compared against a risk assessment performed by human experts. The comparison is done based on the number and diversity of the detected hazards, the effectiveness of the risk analysis in terms of the ability to precisely locate risks instances along the process and of triggering individual risk mitigation actions, and the amount of effort and time required in either of the approaches. More details will be provided during the oral presentation. SAFER-HRC is validated if it identifies at least all hazards detected by human experts with comparable estimated risk values regardless of the scoring method, and mitigates them with similar RRMs.

This work was partially supported by Fondazione Cariplo and Regione Lombardia through the AUTOVAM project.

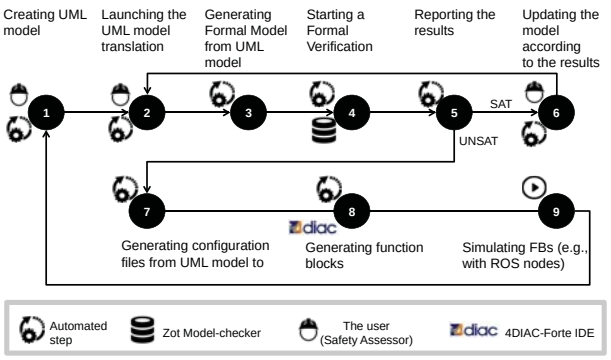

Figure 1: SAFER-HRC walk-through. Fully automated steps alternate with steps that require interaction of the user with the tool (depicted with dual symbols).

The test-case system (shown in Figure 2(a)) is composed of a robot unit that autonomously relocates to either of two assembly stations (1) and (2), or to a sensor-based inspection station (3), a human operator who is mostly present in stations (1) and (2), and another human who works mainly in (3) or executes auxiliary manual tasks on the workbench in (4).

The main robot-assisted intended tasks are: pallet assembly at stations (1) and (2), including bin-picking from local storage carried by the mobile unit; pallet disassembly (reversal of assembly) at (1) and (2), including bin-dumping; pallet

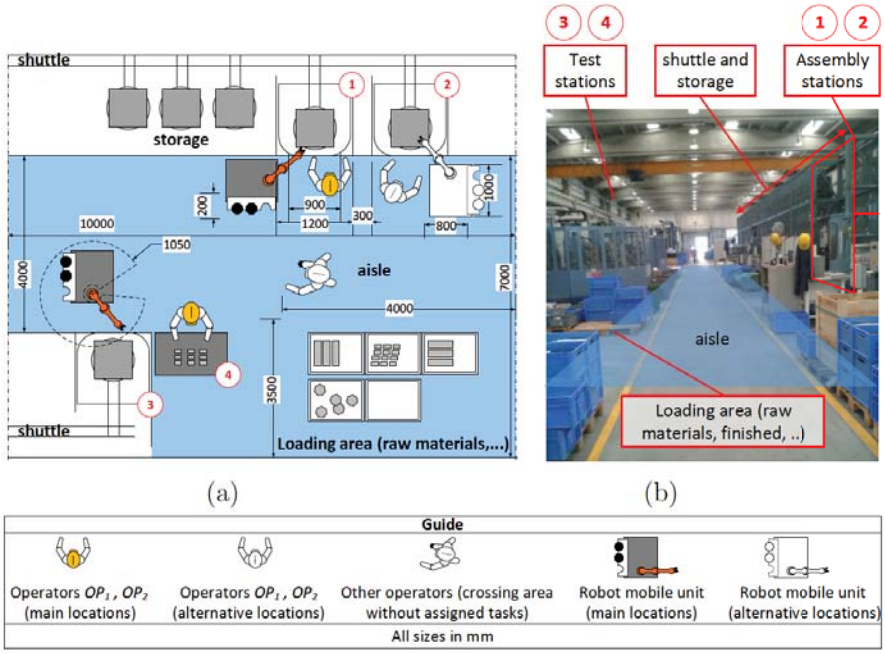

Figure 2: (a) precise workcell depiction, (b) actual layout.

	Hazard Identification										Risk Reduction		General
	# hazards total (individual)	# hazard types	# hazards/links combinations	# Qs hazards	#Tr hazards	multiple instances	# locations	# exposed body parts	support unintended use	rate of intended use	# RRM types	# hazard/RRM combinations	Total required time
manual	31 (19)	2	9	14 (45%)	17 (55%)	no	4	10	yes	48%	6	14	32-40 man-hrs
tool-based	60 (27)	2	8	16 (27%)	44 (73%)	yes	44	5	yes	55%	5	20	20 man-hrs

Table I: Results of the comparison between manual and tool-based risk assessment in hazard identification and risk analysis.

inspection at station ③; lead-through programming of assembly/disassembly/inspection tasks (trajectories, parameters, etc.) at stations ①, ② and ③; material handling on load/unload areas. Frequently, robot base and operators move side-to-side across the central aisle, or other operators transit along the aisle because the target area is part of a larger plant and access to it is not restricted.

Table I shows a comparison between a risk assessment done manually, and another one using our proposed methodology and corresponding tools. More details will be provided during the oral presentation.

References

[1] M. Askarpour, D. Mandrioli, M. Rossi, and F. Vicentini, "SAFER-HRC: safety analysis through formal verification in human-robot collaboration," in *Computer Safety, Reliability, and Security (SAFECOMP)*, ser. LNCS, vol. 9922, 2016, pp. 283–295.

[2] ——, "A human-in-the-loop perspective for safety assessment in robotic applications," in *Perspectives of System Informatics*, ser. LNCS, vol. 10742, 2018, pp. 12–27.

[3] C. A. Furia, D. Mandrioli, A. Morzenti, and M. Rossi, *Modeling Time in Computing*, ser. Monographs in Theoretical Computer Science. An EATCS Series. Springer, 2012.

[4] "Zot: a bounded satisfiability checker," Available from `github.com/fm-polimi/zot`.

[5] L. Lestingi and S. Longoni, "HRC-TEAM: A model-driven approach to formal verification and deployment of collaborative robotic applications," Master's thesis, Politecnico di Milano, 2017.

[6] M. Askarpour, D. Mandrioli, M. Rossi, and F. Vicentini, "Formal model of human erroneous behavior for safety analysis in collaborative robotics," *Robotics and Computer-Integrated Manufacturing*, vol. 57, pp. 465 – 476, 2019.