Matti Vuori, 2014-02-10

Report for ATAC and RATA projects

Testing of human-like robots

Contents

1. Introduction

Human-like robots are expected to be a common sight in workplaces, institutions and households in the future. This is a new type of advanced, intelligent automation. In order to drive the science and craft of testing further, it is now a good time to assess the testing challenges of such products and to build readiness for testing even the most demanding of those – and for the research community to start researching the new issues. This paper discusses just some of the relevant issues.

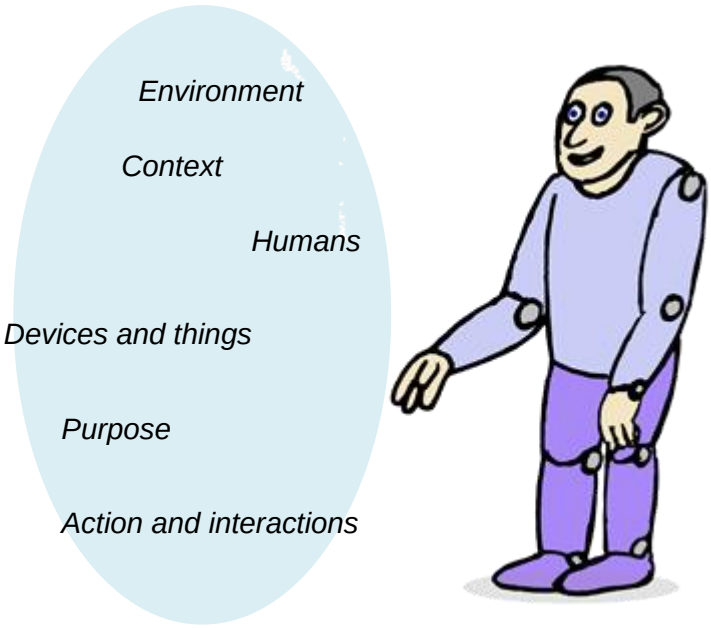

Figure 1. A human-like robot.

2. Characteristics of such robots

Of course there will be many types and configurations of the robot, having very different characteristics:

- Some targeted to be simple physical aid, able to do simple tasks – like lift things for the elderly, or a vacuum cleaner robot.
- Some targeted to be a communications and memory system for the user.
- Some are meant to be for various kinds of personal company and pleasure.
- The size may vary (midget-size is still human-like).
- Some are clearly safety-critical more than others.
- Autonomy will vary – executing simple commands versus doing tasks independently.
- Ability to learn will vary. Some are programmed by the user or the manufacturer or someone else, but some can learn new things itself.
- Etc…

For the sake of assessing a "worst case" – or a "best case" – we will here consider the most advanced do-it-all robots.

Table 1. Characteristics of human-like robots and their influences.

Characteristic	Influence
Is a new thing	People have different expectation about them and there will be surprises.
Is human-like	May lead people to expect an unrealistic level of human-like understanding from them. Causes unfounded trust. Thus makes life more pleasant, but may cause problems with unproven technology. First guidance from when robots were introduced was: do not humanize them, remember that they are machines.
Is physical and moving	Has presence, may cause hazard by moving or blocking movement of humans.
Can lift, move things	May cause hazards by acting on wrong things or dropping things or taking them to a wrong place.
Has an advanced sensory system	Can recognize things much better than any living thing and can communicate in many ways
Is intelligent	Intelligence will be a great aid, but can be dangerous.
Can have personality	Despite the warnings above, a robot clearly can have a personality and that always means some quirks.
Is a software system	The robot's behaviour is based on software. Software makes them suitable to a task and context, and differentiates different robot.
Is networked locally and with the world	The robot can "know everything" – and also reveal everything.
Is technologically diverse and complex	The things are hard to develop and test.

The sensory system is interesting. A robot like this will have many sensors:

- Sound / voice.
- Vision (motion, shape detection), augmented reality (as virtual sensor). Potentially infrared or ultraviolet cues or guidance invisible to humans (as robots become common, environment may be designed to support them).
- Positioning, location.
- Distance meter.
- Speed, acceleration.
- Posture, rotation.
- Proximity.
- Touch.
- Force, pressure.
- Smell.
- Near field data sensors.
- And many others…

Any actions it takes are based on many sources and mechanisms:

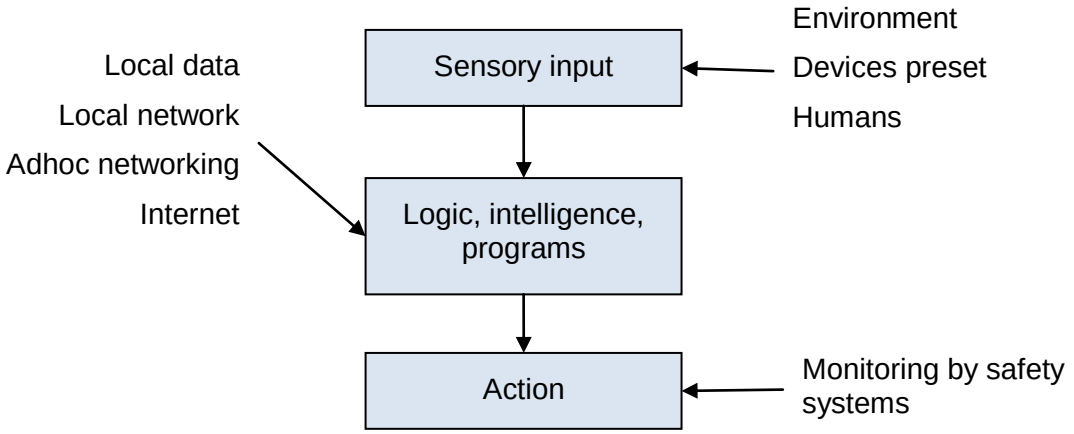

Figure 2. A very simplified process of a robot taking action.

Another model on the process could be like this (based on a sketch by Antti Jääskeläinen):

Inputs		Methods		Possibilities
Contained data, models	→		→	Robot's initial model of the world
Sensor information	→	Logic	→	Updated model of the world
Potential actions in situation	→	Rules, checking guards	→	Possible actions known
Benefit / value functions			→	Estimated value gained from possible actions, associated with the actions
		Logic (heuristics etc.)	→	Selection of action – known, which one is the "best" to execute
		Execution	→	Action

There will be other approaches and the technologies and architectures that they are implemented with will vary.

The whole environment where the robots operate is interesting. In that things happen in parallel, in non-deterministic manner. The whole system is practically unknown and changes often as new devices, people and robots join and leave the collaboration. All participants communicate in diverse ways and may have various roles in any activities (starting them, participating actively, monitoring etc…). Also, some of the elements may and will be malicious and their reliability will be unknown. That calls for "paranoid" security and robustness strategies both in design and testing.

Various types of networks for a basis of the communication between robot, other actors and data storages – or knowledge bases. They include:

- Robot's internal close range network that connects its elements.
- Ad-hoc connectivity with devices and devices in humans (like smart clothing, smartphones etc.).
- Local area network.
- Wide area network.
- Any special networks for special purposes.

As there are many things in interaction, one immediately thinks that to understand, design and test such system a system model of the whole is needed, which in the context of testing leads to thinking that model-based testing is a natural approach to the automated testing of the whole.

3. Testing of the characteristics and elements of the robots

The next table outlines the most essential testing types for the system elements (the list will not contain everything). Note that in this kind of presentation, the system elements are not independent – for example the control system cannot be separated from sensory system and the "intelligence system". Also note that here we discuss the software and behavioural aspects and not much the testing of the physical robot.

Table 2.Testing of various elements of the robot system.

Element	Test types (most essential)	Special challenges
Overall system (robot in action, in environment, in collaboration, as part of systems).	Concept testing (analysis, simulation, mock-ups).	Validating that the robot concept is best one for the context, goals. Validating that the robot has a cultural fit to where it will operate.
	Functional testing.	For automated testing: Environment simulation, programmatically created user gestures, voice commands… For MBT: Modelling of environment (elements and behaviour) – including devices and humans. Use cases / stories for both humans and the robot. Exploratory testing important due to complexity. Testing the operating logic in a simulated environment vs. testing the physical robot in the real world. Changing environment setup. Need a paranoid approach to how other system elements behave.
	Safety testing.	Need a thorough risk / safety analysis for basis. Testing requirements from safety standards – advocate advanced techniques, such as MBT. Safety is related to security too – dangerous remote control…
	Security testing.	Low level of trust in any system elements.
	(Regulatory) validation testing.	Unclarity of the regulations and their interpretation, unclarity of what standards are appicable.
	Performance / capability testing.	–
	Compatibility, co-existence testing.	Testing of the diverse technologies and variations in the collaborating environment.
	User experience testing.	Need to assess overall relation between human & robot – is as planned?
	Localization testing.	Whole behaviour, meaning of control gestures, behavioural rules – it can really be cultural testing of cultural fit (by no means checking of translations…).
	Upgradeability.	Testing of updating software or hardware.

Element	Test types (most essential)	Special challenges
Control system	Functional testing.	Testing of movement in practical spaces.
	Reliability testing.	Reliability analysis as basis.
Intelligence systems	Testing of logic, decisions.	All deviations, non-determinism, context data.
Sensory system (perception system)	Functional testing.	(Depends on sensor). Variation on input – gestures, sound, ambience…
	Reliability testing – defective sensor etc…	–
Safety system	Functional safety testing.	Testing requirements from safety standards (such as SFS-EN 61508 series) – can be very demanding! Needs safety / reliability analysis for basis.
Communications system (technical)	Functional testing.	–
	Reliability testing.	–
	Performance testing.	Including load, stress testing.
	Security testing.	–
Human interface (user)	Usability testing, analysis.	The new ways of interaction can be difficult to validate.
	Analysis and testing of human errors.	Must test for human errors thoroughly (voice, gesture commands).
	Obedience testing.	Who is in control, when many humans are present (or TV is on).
	Functional testing.	Exploratory testing is critical – need to have almost a “psychological” approach.
Human interface (programming & configuration)	(As for user interface).	
	Security testing.	Who can program / configure? Consider remote control.

4. Notes on the psychology of testing and competence

Testers are humans and as such they are prone to the same psychological phenomena as the users of the robots. They may tend to treat the human-like robots with awe, respect and care. But that is the enemy of good testing. Good testing should aim to breaking the software (though not to breaking the physical robot…) and that obviously requires that we do not care about its well-being. The more in trouble the human-like robot gets in testing, the better! So we need pay attention to the testers’ attitudes.

Another phenomenon is that people extrapolate their testing approach from history and previous projects in “just enough” manner – is nobody complains about the inadequacy of the approach, it must be ok. But when the systems under test take a leap in challenges – new concept, new level of complexity, new types of systemic interactions, large amount of new technology, a mix of different development cultures – the whole testing should be reassessed. It would be an error to think them as just another programmable device, yet another type of automation or a more serious toy.

All this requires better than normal testing competence, preferably more than one tester with complimentary competences. For example UX testing competence – not just usability testing – and understanding of automation systems and safety-critical systems are especially essential to have in the core team. Security analysis and testing skills can often be "outsourced". The hardware-related testing competences will depend on the nature of hardware development and sourcing. In a context like this, an important meta-competence is the ability to understand what kinds of competences are needed in the development and testing and to be able to reflect own competence against that.

One of the functions of testing is learning about the things that are developed. In this kind of setting that is especially important. So good testing here cannot be "execution", but an attempt to understand the new things, to gain insights to act upon.

5. Summary

Based on the brief analysis, the robots have some interesting characteristics, which can be demanding for the testing. There is a need for testing research, methods development and perhaps for some regulation too, such as safety standard tailored for this kind of systems.

There will be robots of many kinds, and the high-end models will be the most problematic, because they combine advanced, complex product technology with advanced, complex interaction with humans and environments, causing possible risks of many kinds. They will be the hardest to test properly and hopefully will get the attention to quality and safety they – and their users – deserve.

6. References

SFS-EN-61508-1. 2nd edition, 2011-01-24. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1: General requirements. (Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 1: Yleiset vaatimukset.) 117 p.

SFS-EN-61508-3. 2nd edition, 2011-dd-pp. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1: Software requirements. (Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 3: Vaatimukset ohjelmistolle.)