Matti Vuori, 2013-10-16

Remote robot testing system review checklist

This is a generic checklist for reviewing a remote robot assisted test system and to support designing of such. List focuses on the arrangements for remote testing and less on the testing features. Potential users of the list include purchasers and test system developers. Note that many of the required and expected features and safety characteristics of the system will depend on for example its performance / forces and other parameters. For any particular test system type, this list can be tailored to suit.

1. Safety of the electromechanical system

- The robot is designed to be safe in industrial level.
- The status of remote operation is clearly visible locally.
- The status of local operations is clearly visible remotely.
- During remote operation the robot arm mechanics and other moving parts cannot be accessed.
- Accessing the robot locally interrupts the remote operation in safe manner. For example, the robot arm does not move according to remote scripts or move “home” after opening a cover to access it.
- The system is provided with a safety switch.
- The remote system has an electronic safety switch and facilities for creating an alarm locally.

2. Communications security

- Remote connectivity is sufficiently secure, considering the secrecy of products under test.
- All elements of communication are secured, including scripts, video feed, collection of logs, possible chat systems, meta-information about sessions (for example, who is currently testing) etc.

3. Local security

- Robot premises are sufficiently isolated with appropriate access control.
- The robot testing ICT infrastructure is isolated for the hosting company’s other systems appropriately (for example no access to client’s proprietary device data, test data or test logs).

4. Observability – visibility of activity and problems locally and remotely

- The robot environment can be monitored remotely.
- There is a good view to the state of the robot and the test system during test runs.
- Outside of test runs there are arrangements to reserve the system it is free so that there are no conflicts between other potential remote or local users.

5. Reliability

- The system is sufficiently reliable for remote use. For example, it does not require any adjustments during test runs.

6. Recoverability from problems

- The system can be restarted remotely after any system problems.

7. Local support arrangements

- There is a local operator available during the session.
- The local operator has monitoring facilities for the robot.
- Contact information about the current operator is informed to the users of a remote session. In practice: who to call when there is a problem. The remote monitoring system should also have tools for alarming the local operator.
- Full information about the remote session is clearly presented for the local operator.
- There is a clear contract on the service level.

8. Documentation for users

- The system has good functional documentation for the remote tester.
- The system has “code of conduct” for remote testing that the customer must “sign” and adhere to.
- The system has safety and security instructions for remote use. The customer is sufficiently educated on these issues.

9. Preparation for testing

- There are provisions for simulating test runs remotely without the robot or remote connection to see that the test scripts behave as designed and expected. (For example a software-based robot emulator / simulator.)
- There are “sanity checks” in the test system that can already be used in the simulations that can catch for example catch request that cannot be fulfilled, e.g. tapping an area that is out of the tappable device are.

10. Design process of the system – design for safety, security and reliability

- Design requirements:
    - A risk and safety assessment has been made to the system.
    - A reliability assessment has been made to the system.
    - A security assessment has been made to the system.
- The system fulfills any appropriate (local and remote) safety regulations and standards.
- The system is designed for safety and robustness and for example monitors its control requests for problematic actions (harm for device, too rapid movements, potential for oscillations).

11. Configuration control

- All changes in the system and its control interfaces that may cause changes in its behavior are communicated to the remote users.
- There is an up-to-date documentation of the remote behavior with change information.

12. Other

- *Other things to consider in this particular system?*