PROPERTIES OF TKA SYSTEM:

As expected with a medical cyber-physical system, the range of properties collected in the ExactechGPS-TKA case study is very wide. In this section, we present a set of properties that we identified as representative. Here is the list of the 15 properties in no particular order:

Property 1: The trace contains a step “redo acquisitions”. The “redo acquisition” step allows the surgeon to correct his previous acquisition. It is not part of the standard procedure flow and, therefore, interesting to detect.

ParTrap : *occurrence\_of Enter e where e . state == 'redo '*

Property 2: The temperature of the camera stays within [l, u]. If used in proper conditions, the camera temperature should not deviate from the range where its precision is guaranteed.

ParTrap : absence\_of Temp t where not ( a <= t . t1 and t . t1 < b)

Property 3: The distance between pairs of hips centers is less than d. This property asserts that the algorithm computing the hip center is stable.

after each HipCenter h1 , absence\_of HipCenter h2 where dist ( h1 . point , h2 . point ) >= d

On prend le premier HipCenter

Property 4: The distance between the hip center and the knee center is greater than d. A violation of this property could reveal an abnormal positioning of the patient or the sensors.

Property 5: If the medial malleolus is further than the lateral one, a warning is issued. A violation of this property could reveal that the 3D camera was installed on the wrong side of the patient.

set ( MedialMalleolus m, LateralMalleolus l) where

norm (l. point ) < norm (m. point ) followed\_by WarningMalleolusInverted

Property 6: The user never skips a screen. The surgeon is expected to spend sufficient time to appreciate the information showed at each step of the procedure.

Enter prevents ActionNext for 100 ms

Property 7: The acquisition of a point succeeds if and only if the probe is stable. If the surgeon moves the probe during an acquisition, it should not be accepted.

AcquirePoint ap where isStable (ap. cloud ) followed\_by PointAcquired

Property 8: The protocol “redo acquisitions” proposes only already performed acquisitions. The system should not offer the user to redo acquisitions that were never performed.

before each Redo r, forall o in r. options ,

occurrence\_of Enter e where e. state == o

Property 9: Detecting a new tracker produces a dialog asking for replacement confirmation.

after each RegisterTracker rt ,

TrackerDetected td where td. type == rt. type followed\_by

DialogConfirmReplace dc where dc. type == rt. type

Property 10: The state TrackersConnection is unreachable until the camera is connected. The system should not reach a state dependant on the camera until the camera is connected.

Enter e where e. state == 'TrackersConnection ' preceded\_by CameraConnected

Property 11: A replaced tracker is not used until it is registered again. If a tracker is replaced, the system should not try to use it until it is registered again.

since ( Unregister u) until ( Register r where r.id == u.id),

absence\_of ( Activate a where a.id == u.id)

Property 12: The action “previous” cancels the current points cloud acquisition. Acquiring a points cloud takes a few seconds and can be cancelled. In this case, the current acquisition should not succeed.

since AcquisitionCancel until AcquisitionBegin ,

absence\_of AcquisitionSuccess

Property 13: All the necessary trackers are seen before entering the state TrackersVisibCheck. To proceed, the system requires a set of trackers depending on the profile in use. All these trackers should be seen at least once before entering the state TrackersVisibCheck. Note that if we go back to the beginning and change the profile, the trackers already seen do not have to be seen again.

before each EnterState e

where e. state == " mainCasp . TrackingConnection . TrackersVisibCheck ",

given last SearchTrackers st ,

forall ty in st.types ,

occurrence\_of TrackerDetected td where td.ty == ty

Property 14: On the tracker’s connection screen, a tracker is shown if and only if it is necessary. Only the set of required trackers is shown to the user.

since SearchTrackers st1 until SearchTrackers ,

absence\_of ScreenshotTrackersConnection stc

where stc. trackers != st1. requiredTrackers

Property 15: In the state TrackersConnection, not detecting any new tracker for 2 minutes produces an error message.