Node Health Monitor

Scope

The Node Health Monitor is part of a suite of components that manage the lifecycle of an Infotainment HeadUnit. The Node Health Monitor (NHM) keeps track of the ECU current state and coordinates the system lifecycle from bootup to shutdown. It defines the main interfaces for controlling a given application during the lifecycle, and provides the facility for applications to react to important system events. The specific logic is different for every system which is why there is a plug-in containing the specific state machine for each particular system, i.e. the Node State Machine.

git repository for NHM code: http://git.projects.genivi.org/lifecycle/node-health-monitor.git

Node Health Monitor

The Node Health Monitor is part of a suite of components that manage the lifecycle of an Infotainment HeadUnit. Health Management ensures that the node runs in a stable and defined manner. To do this it provides the following multi-layered observation system and escalation strategy.

The Node Health Monitor will work in conjunction with systemd to monitor component failures in the system. It will be responsible for :
a) monitoring systemd to automatically record and track failures per component (i.e. application, service)
b) providing an interface with which components can register failures when not using the systemd monitoring
c) maintaining failure statistics over multiple lifecycles for the system and components (the service name will be used to identify and track component failures)
d) maintaining statistics on number of failures in number of lifecycles (i.e. 3 failures in last 32 lifecycles)
e) monitoring the wakeup and shutdown events to catch unexpected system restarts
f) provide an interface for components to read system and component error counts
g) provide an interface for recovery clients to request a node restart

Additionally the Node Health Monitor will test a number of product defined criteria with the aim to ensure that userland is stable and functional. For instance it will be able to validate that :

there is enough free system memory
the CPU is not reporting an excessively high load for a sustained period
defined file accessibility is possible
defined processes are still running
communication is possible (D-Bus)
a user defined process can be executed with an expected result

If the NHM believes that there is an issue with user land then it will be capable to initiate a system restart

Recovery Clients

A “Recovery Client” is a component that is executed when a failure has been detected in the system. There can be a one to one relationship between apps and recovery clients or one client can handle multiple apps. It should contain enough functionality to be able to :

request the error status count from the NHM (based on name of the service file failing)

based on the error count, escalate the recovery action, for instance:
file system mount failure, recovery action could be to format the file system and request a node restart
if it is an application that has failed multiple times then we may want to delete that applications persistency data and restart the application
when possible, request that the SW is uninstalled or rolled back to a previous version

request systemd to restart the application

request a node restart via the NHM

The Node Health Monitor (NHM) keeps track of the ECU current state and coordinates the system lifecycle from bootup to shutdown. It defines the main interfaces for controlling a given application during the lifecycle, and provides the facility for applications to react to important system events. The specific logic is different for every system which is why there is a plug-in containing the specific state machine for each particular system, i.e. the Node State Machine.

See also

Node State Manager

Transferred from MediaWiki. Original author and history:
Created: 11:33, 14 May 2014 Jeremiah
for Latest changes -> View Page History in this Wiki