AC75 Interpretation 018

of

AC75 Class Rule Version 1.2 issued 10th December 2018

Rule References:

26.2 The **CIS**:
(a) shall be incapable of measuring any part of the **yacht state**;
(b) shall not be capable of having any significant effect on the **yacht state**;
(c) may use short range wireless communication in **crew indication devices** and associated interface hardware (e.g. access points); and
(d) may include microphones and speakers to allow direct voice communication between crew, and to play audio signals from **CIS** devices.

26.3 As an exception to Rule 23.5 (b), **crew indication devices** in the **CIS** containing sensors such as accelerometers or solid-state gyroscopes may be considered incapable of measuring any part of the **yacht state** if a **Competitor** can demonstrate to the satisfaction of the **Measurement Committee** that those sensors cannot be accessed, for example by installation of custom firmware verified by the **Measurement Committee**

Background:

We consider a device such as a smartphone or a tablet used as a **Crew indication device.** These devices can contain sensors such as accelerometers, gyroscopes, magnetometers, pressure sensors, light sensors, proximity sensors, cameras, humidity sensors, temperature sensors, and GPS (or other global positioning systems).

Attention is drawn to the attached paper which explores the access to devices inside smartphones and tablets, and while not directly linked to disabling specific sensors, it provides insights into possible solutions to limiting the capability of the device whilst racing. https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-petracca.pdf

Questions:

1. Is such a device, if worn by a crew member, considered to be capable of measuring part of the yacht state? If so which of the sensors mentioned above infringe Rule 26.2?

2. Is such a device, attached to the yacht, considered to be capable of measuring part of the yacht state? If so which of the sensors mentioned above infringe Rule 26.2?

3. If such a device is considered capable of measuring the yacht state, is logging of the device sensors usage sufficient to prove that no application has accessed sensors while racing which could be capable of measuring any part of the yacht state?

4. If such a device is considered capable of measuring the yacht state, are permission restrictions of the device's operative system enough to satisfy Rule 26.3. Such permission restrictions would prevent an application accessing prohibited sensors.

5. If such a device is running a custom operative system that doesn't provide access to the sensors capable of measuring part of the yacht state, would it be enough to satisfy Rule 26.3?

If such a device, capable of measuring part of the yacht state, is used in a kiosk lockdown mode, would it be enough to satisfy Rule 26.3. In such mode the device would always boot the same application, approved by a

third party, that provides a sandbox, without access to the sensors. The user cannot exit that application without entering a password that would only be known by the measurers. Further examples of kiosk lockdown are provided in the websites below.
https://www.42gears.com/products/surelock/
https://www.android-kiosk.com/
https://www.hexnode.com/mobile-device-management/android-kiosk-browser/

6. Would Rule 26.3 be satisfied if tamperproof software was installed on a device, which prevented access to internal sensors which could measure yacht state.

7. Would a declaration from a software developer(s) of the application running on a device be enough to satisfy Rule 26.3. Such declaration would state that no access is provided to sensors which could measure yacht state.

8. Would the installation or/and compilation of the application under the supervision of a measurer be enough to satisfy Rule 26.3. The measurer would have the opportunity to inspect the source code as well as being provided with means to check, at any time, that this version of the application is the one running on the device.

Interpretation:

Not applicable.

Answers:

1. Yes. Accelerometers, rate sensors, gyroscopes, magnetometers, pressure sensors, proximity sensors, cameras, humidity sensors, GPS, infringe Rule 26.2.
2. Yes. Sensors as listed in 1, except as specifically allowed by the AC75 Class Rule such as Rule 23.1(c) regarding standalone **hardwired** cameras mounted on the **yacht.**
3. No.
4. Only if the operating system (firmware) is a custom version which permanently restricts access to prohibited sensors, and which cannot be replaced.
5. Yes, if the custom operating system (firmware) permanently restricts access to prohibited sensors, and cannot be replaced.
6. Yes, if "tamperproof" is understood to mean a custom operating system (firmware) that cannot be replaced.
7. A restricted application is not sufficient to satisfy the rule. A declaration from of a software developer(s) of custom firmware that restricts access to prohibited sensors and cannot be replaced would be part of an acceptable solution.
8. A restricted application is not sufficient to satisfy the rule. The installation, under measurer control, of a custom operating system (firmware) that restricts access to prohibited sensors and cannot be replaced would be part of an acceptable solution.

Further to the above, "cannot be replaced" is satisfied either by BIOS changes that prohibit further upgrades, or by hardware modifications provided that those hardware modifications permanently prohibit BIOS changes.

END