Verification and Validation of Autonomous Systems Software

We have come to depend, both as individuals and as a society, on software. From smart phones to power stations, airliners to e-commerce, our economy and society is increasingly dependent on software running on a variety of devices. However, these devices will become increasingly autonomous performing everyday tasks from domestic chores to driverless cars. The trustworthiness of the software is thus an underlying concern for those who commission, write and use it.

A recent BSI publication (PAS 754:2014 see reference [1]) identified five aspects of software trustworthiness: safety, reliability, availability, resilience and security. For example, how do we ensure that an autonomous drone can safely deliver your latest paperback without injury to persons or possessions? And how can we ensure it is secure so that a hacker does not receive your book instead?

Given the wide variety of devices and software under consideration, the BSI document describes a widely applicable approach to achieving software trustworthiness rather than mandating any specific practises or procedures. For example, the standard bases the approach on the following concepts:

- Governance. Before producing or using any software which has a trustworthiness requirement, an appropriate set of governance and management measures shall be set up.
- Risk assessment. The risk assessment process involves considering the set of assets to be protected, the nature of the adversities that may be faced, and the way in which the software may be susceptible to such adversities.
- Control application. Risk shall be managed through the treatment of risk by the application of appropriate personnel, physical, procedural and technical controls.
- Compliance. A compliance regime shall be set up to ensure that creators and users of software ensure that governance, risk and control decisions have been implemented.

These concepts are not new. For example, we have been concerned with safety in other domains for many years. The software and electronics on board aeroplanes is controlled by existing standards (such as DO254 and DO178C) which defines the development approach, principles and deliverables. Similarly, ISO26262 has been created recently to create a compliance regime for the development of the software and electronics that we increasing find in our cars. Security in software applications is covered in ISO/IEC 27034 Application security standard. In the future, however, such levels of trustworthiness will be required in a much wider variety of devices that operate autonomously.

So, the aim of all this Verification and Validation activity is to ensure that the first time you get into your driverless car you can feel both safe that it will not crash and secure that nobody has altered your destination address. Or, more near term, when can you return home each day and trust that your autonomous vacuum cleaner has left your house in a tidy state!

References:

1. PAS 754:2014 "Software trustworthiness Governance and management Specification"