IoT Transport and Mobility Demonstrator

Cyber Security Testing on National Infrastructure

Policy Recommendations

Miles Elsden*, Carsten Maple‡, Matthew Bradbury‡

* Elsden Consultancy Services Limited, ‡ Warwick Manufacturing Group, University of Warwick

May 2019

WMG Policy Recommendations

As part of the PETRAS project demonstration phase IoT-TRaM project[1] a range of cutting edge IoT cyber security approaches where tested on a number of UK CAV testbeds currently under development as part of the DfT/UKRI/Zenzic funded CAV testbed programme. The UK ambition is, as well as providing individual test capabilities, to develop a coherent UK CAV testing offer. This would support the testing of sub-systems, vehicles and system level applications across the full range of testing scenarios from lab-based to real-world deployment.

The current generation of test sites are at various levels of maturity though they were mostly at the design or early deployment stages during the PETRAS demonstration programme. The PETRAS 'Moving in the Internet of Things' demonstrators provided an early opportunity to learn lessons around some of the key challenges to developing and deploying viable testing environments.

A number of common lessons were identified for both users and test site operators that have application across all sites. Specific lessons for users and operators are presented elsewhere[2]. This report looks at issues where intervention at a strategic level would be valuable to support the vision of a clear, coherent UK CAV testing eco-system. These fall into three broad categories: Modification of hardware/software, Communications and Digital Twins, as well as a small number of more general recommendations.

Software/Hardware Modification

Existing, commercial off-the-shelf (CoTS) on-board (OBUs) and road-side units (RSUs) are based on existing communication and security standards. These are sufficient for early testing, but it is clear they are insufficient for widespread role out of CAVs. They are not able to support many of the next generation of security, privacy and trust techniques currently under development (such as those developed under PETRAS). To be able to implement and test these new approaches researcher and test-bed users need to have the ability to modify aspects the software on the deployed hardware. This capability is generally made available by the manufactures through Software Development Kits (SDKs) or equivalents. However, manufactures understandably want to control access to this capability.

During the PETRAS tests getting access to the necessary SDKs presented some issues. This is likely to be a common need across most users and for all test-beds. There will be clear advantages from UK wide discussions with key manufactures to agree access to the necessary SDK (or equivalent) tools. Given its role, Zenzic would be best placed to take this role.

Recommendation: Zenzic should negotiate with key hardware suppliers to get agreed access for all users and test-sites to the necessary Software Development Kits (SDKs) or equivalent.

[1] https://www.petrashub.org/iot-tram-enabling-more-secure-connected-and-autonomous-vehicles/

[2] Carsten Maple et al. "IoT Transport and Mobility Demonstrator: Cyber Security Testing on National Infrastructure." Technical Report, University of Warwick, May 2019

More widely, users are likely to need to deploy custom firmware versions on a broad range of V2X devices to support new, novel security approaches. While necessary for testing of a range of new technologies, there is also a risk from the introduction of maliciously or inadvertently insecure devices into the network. Developing a consistent approach across all the testbeds would support the ambition of users being able to move seamlessly between test environment and locations.

Recommendation: Testbeds should develop and agree a secure and consistent approach to the deployment of custom firmware images on the widest range of V2X devices.

Communications

The rules concerning communications licenses for different bands and communication protocols is complex, particularly if testing non-EU compliant communication devices in the UK. Consideration should be given to making this process as straightforward as possible. Zenzic/C-CAV should discuss with Ofcom whether certain types of security testing with known V2X hardware can be conducted without requiring a licence. In general, clear information on what communication deployments are exempt and which require a licence (and the process for obtaining any necessary licences) should be made available.

Recommendation: Zenzic or C-CAV should agree with Ofcom what licences are needed for CAV testing and whether some of the existing requirements can be relaxed. Zenzic should supply clear, easily accessible information on licence requirement for current and proposed V2X communication technologies and clear guidance on how to apply for test licences.

Digital Twins

All UK testbeds are required to have a level of Digital Twin capability. While the meaning of ‘Digital Twin’ is not yet agreed, having a consistent and interoperable approach to testbed Digital Twins would be a key offer as part the single UK testing vision. Zenzic is keen to ensure that the Digital Twins across the different test-sites provide this interoperability (while respecting the commercial interests of the individual test sites).

From the PETRAS work there are a number of aspects of Digital Twin interoperability that should be considered. Three areas where identified as part of this that should be considered for inclusion in future work on ensuring consistency of digital representations across the testbeds.

Firstly, there needs to be the ability to share code between the simulation environment and the deployed hardware (this is related to the SDK point above). Environments should be encouraged that allow porting of code between software simulations, test harnesses and deployed hardware to reduce the costs and risks of re-writing code for different environments.

Secondly, any agreed data standards should support the widest range of popular simulation tools used in academia and industry. These data formats should be well specified and conform to industry standard approaches wherever possible. The development of a freely available translation tool should also be considered as part of future Digital Twin work.

Finally, an accurate representation of the RF characteristics of the test-sites should be made available that can be easily integrated with widely used RF simulation software. Given the dependency of CAV systems on V2X communications, this will be a key factor in the usability of Digital Twin representation of the test-sites, and ensure simulation results can be accurately transposed onto real-world deployments.

Recommendation: Future work on aligning Digital Twins across the testbeds should ensure code sharing across different software and hardware deployments. Interoperability should be based on the use of widely accepted formats and a translation tool should be provided. Digital Twins should also consider the RF characteristics of the test-site and aligning this with standard simulation data formats.

General Recommendations

In addition to the specific recommendation made above, there were a number of more general observations from the demonstrations that it would be useful for Zenzic to take forward.

Firstly, there is the need for clear, easily accessible information on what capabilities are available at the different testbeds and under what environment - such as GNSS jamming in a controlled environment or DoS simulation capability in a real-world setting. This would enable potential customers to clear map their testing needs across the UK testing eco-system. This would also enable Zenzic/C-CAV to identify gaps and overlaps in testing capability as requirement develop. This should include a clear list of Points of Contact for each test-site.

Recommendation: Zenzic should develop and maintain a catalogue of UK test sites and their capabilities that can act as a one-stop-shop for users to understand what testing can be performed where, and support development of a coherent end-to-end testing plan.

Finally, a consistent approach to Risk Assessments should be supported across all the UK testbeds. This will need to be augmented by site and test specific risks but having a pre-populated baseline Risk Assessment that is consistent across all test-sites would be extremely valuable. This should be supported by clear, consistent guidance on how additional risks would be assessed.

Recommendation: Zenzic work with the existing testbeds to develop a common core Risk Assessment document and develop agreed guidance on how site or test specific additionality would be managed.