PNT Cyber Resilience: a Lab2Live Observer Based Approach

Report 2
Specifications for Cyber Testing Facilities

Matthew Bradbury, Elijah Adegoke, Erik Kampert,
Matthew Higgins, Tim Watson, Paul Jennings,
Colin Ford, Guy Buesnel and Steve Hickling

April 2020

Research Undertaken By

Research Supported By

Research Funded By

Cite this document as:

M. Bradbury, E. Adegoke, E. Kampert, M. Higgins, T. Watson, P. Jennings, C. Ford, G. Buesnel, and S. Hickling. PNT Cyber Resilience: a Lab2Live Observer Based Approach, Report 2: Specifications for Cyber Testing Facilities. Technical Report 2, University of Warwick, Coventry, UK, April 2020. Version 1.2

Executive Summary

The use of global navigation satellite systems (GNSS) such as GPS and Galileo are vital sources of positioning, navigation and timing (PNT) information for vehicles. This information is of critical importance for connected autonomous vehicles (CAVs) due to their dependence on this information for localisation, route planning and situational awareness. A downside to solely relying on GNSS for PNT is that the signal strength arriving from navigation satellites in space is weak and currently there is no authentication included in the civilian GNSS adopted in the automotive industry. This means that cyber-attacks against the GNSS signal via jamming or spoofing are attractive to adversaries due to the potentially high impact they can achieve.

This report introduces specifications and recommendations for GNSS cyber-security test facilities for CAVs. These specifications are based on a survey of academic literature, interviews with a select group of experts, and experiences obtained performing laboratory and real-world testing (shown in Figure 1).

Figure 1: PNT cyber resilience feasibility study carried out at Wellesbourne Campus

Key Findings

The three key findings of this report are:

1. Spoofing and jamming attacks on GNSS signals are capable of leading to severe loss of functionality and safety in CAVs by denying them access to or providing them with incorrect positioning, navigation, and timing (PNT) information.

2. PNT testing facilities are urgently needed across a wide spectrum of capabilities, from simulation in artificial environments to over-the-air (OTA) testing in labs and real-world environments. Procedures to legally perform real-world testing via OTA broadcasts need to be developed.

3. There is existing work on the standardisation of GNSS attack detection and GNSS resiliency assessment. Zenzic, UK CAV testbeds, the University of Warwick and Spirent should work with these bodies to guide the development of standards, and to further develop both attack event detection and responsible disclosure of information on threat actors and attack events.

Attack Detection and Mitigation

As described in detail in [2], from the academic literature surveyed, as well as the practical Lab2Live work carried out in the course of the project, it is evident that robust countermeasures for GNSS vulnerabilities are required for CAVs, CAM and ITS. Because it is envisaged that the threat landscape will evolve, nation states must invest in addressing cyber-security as it relates to public infrastructure that relies, in full or in part, on GNSS for operation. With respect to GNSS threats, a wide range of attacks can be carried out both at the physical and software layer. For the latter, software attacks involve sending crafted packets in order to exploit software vulnerabilities in the GNSS receiver's implementation of calculating the position and time from the NAV data sent by GNSSs, which can lead to violations of availability or integrity. For the former, jamming attacks are prevalent in today's transport networks, however, not all occurrences are intentional. Hence, threat actors can employ similar commercially available devices to disrupt a CAV or CAM. Spoofing attacks are also likely to occur, but require advanced knowledge and detailed information about the target, and are thus not yet an immediate threat. Nevertheless, the ability of threat actors will evolve with the proliferation of software defined radio and networking capabilities, hence spoofing attacks do need to be addressed by a future CAV cyber-security test facility. An overview of GNSS attack vulnerabilities is shown in Figure 2.

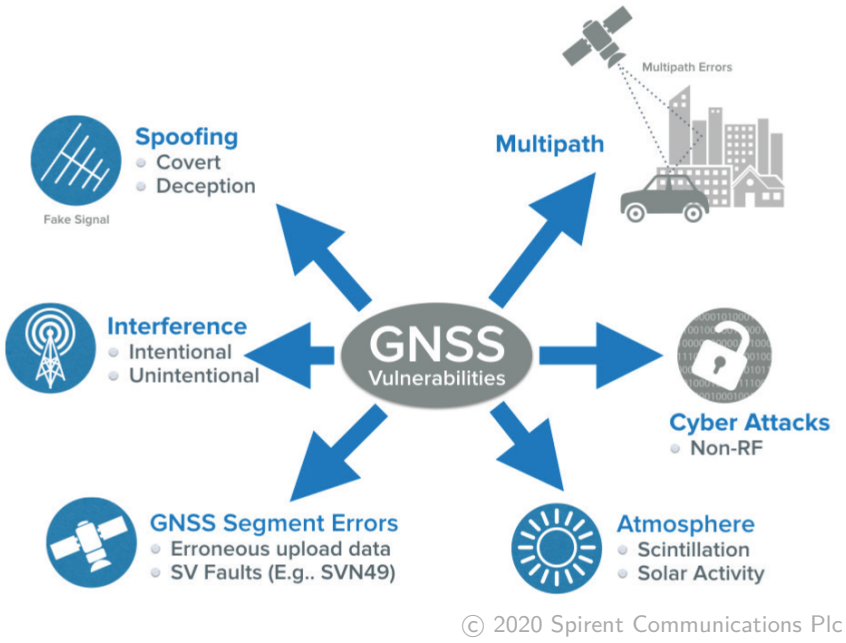


Figure 2: Range of typical GNSS vulnerabilities

Academia and industry are already developing detection and mitigation techniques to enhance the robustness of GNSS receivers. As made evident in [2] and the reviewed literature therein, jamming and spoofing are usually detected and/or mitigated using different techniques, which have different implementation architectures and varying complexity. The approach employed by the CAV or CAM designer can involve mitigation techniques with which the attack is not only detected, but also its effect is minimised. In order to reduce the complexity and enhance the resilience testing, joint mitigation as well as joint detection techniques need to be adopted by OEMs. Testing methodologies for software systems are being developed as well, however, as exhaustive testing of all inputs is impossible due to the large input state-space, important inputs can be identified with a sensitivity analysis and the crafted values to focus testing on can be chosen based on this analysis.

Community Experience

Whereas the academic literature generally focuses on research and innovations, this project also invited a wide range of experts from the automotive, PNT and cyber-security industries to provide their opinions on CAV GNSS resilience and vulnerabilities. This approach allowed the project team to obtain a different perspective from key industry players on how to address vulnerabilities associated with PNT for CAVs and CAM. From the interviews, it was evident that CAV PNT attacks such as jamming and spoofing are credible, the PNT threat landscape needs to be studied as it evolves and the CAV needs to be studied as a system-of-systems.

Testing

A Lab2Live approach to CAV PNT cyber resilience testing has been adopted in this project, yielding complementary results from the lab-based and real-world, live-sky work. A plethora of procedures to execute PNT attack scenarios exists, hence both lab-based and live testing require labour-intense work before all interesting parameters are investigated, and a complete and reliable conclusion on a system's PNT-attack resilience can be provided. In order to carry out the full range of Lab2Live tests, a PNT attack emulator as used in this presented feasibility study is an ideal component of a robust research methodology.

From the lessons learnt and findings of this project, it can be seen that threat actors, attack vectors and countermeasures will evolve. As a result, **government and all associated stakeholders need to continue to work together to foster collaborative research and development that is capable of testing and certifying PNT for CAVs and CAM in the UK**.

Specifications and Recommendations

The knowledge obtained from the expert interviews and the Lab2Live feasibility study were used to develop these specifications and recommendations which are further described in Chapter 4.

Specifications

S 1	A set of standard threat actors who attack GNSS systems should be defined, e.g., by the National Cyber Security Centre, and made available to the testing facility. Tests should then focus on these threat actors. This list should be revised over time as the threat landscape evolves.
S 2	A test facility should support performing tests over the full range of the test continuum, from simulation to emulation to testing in a real world environment. There need to be sufficient capabilities across the UK to support the testing of jamming or spoofing GNSS signals: (i) using GNSS testing equipment via a physical connection to the CAV's GNSS receiver or (ii) an over-the-air attack with a portable GNSS simulator enclosed within an anechoic chamber. If possible, specific test sites should also aim to (iii) support live, outdoor, jamming or spoofing of GNSS signals. This is required to test the feasibility of such attacks in a real-world environment and to further improve the simulations of such attacks.

S 3	The equipment used to perform PNT attack emulation should support technical capabilities that are necessary to perform testing.
S 4	A test facility should provide access to an anechoic chamber to allow legal testing of OTA attacks on GNSS systems.
S 5	A test facility should provide areas in which non-OTA testing can be safely performed in real-world environments. A variety of environments (e.g., urban, rural, motorway) need to be supported to test the environmental impact on an attacker's capabilities and the impact on the implemented mitigations.
S 6	A standard set of metrics should be defined and used to evaluate the resilience of CAM systems when their PNT system is under cyber-attack.
S 7	A test facility needs to be able to support evaluating the resilience of a vehicle against single and multi-sensor attacks.
S 8	A standard test suite of GNSS jamming and spoofing attacks should be defined and made available to organisations performing testing at different test facilities.
S 9	The test facility should supply a group of control vehicles with known functionality and responses to a test suite. This is in order to: • Ensure the test has the same impact on the control vehicle. • Evaluate the possible different impacts on the test and control vehicle.
S 10	A set of appropriate sites need to be identified where PNT attacks can be performed in real-world environments in order to understand and demonstrate the feasibility of an adversary performing these attacks.
S 11	A test facility needs to have contacts with relevant authorities in order to guide the testing performed in terms of the national interest.
S 12	A test facility needs to be able to hold classified information and have the ability to report information such as critical vulnerabilities to the relevant authorities.
S 13	A testbed should provide facilities that support testing of the PNT attack resilience of individual components and multiple interacting systems.
S 14	Employees at a test facility need to have skills in RF, cyber-security and automotive.
S 15	Employees at a test facility need to be suitably vetted, and risks posed by employees and contractors (i.e. insider threat) need to be appropriately managed.

Recommendations

R 1	Vehicles should be tested in various driving modes (if possible): (i) GNSS-only and (ii) fusion of GNSS with other vehicle on-board sensors.
R 2	A set of standards needs to be created to measure the resilience of PNT attacks against CAM systems.
R 3	A test facility should subscribe to GNSS threat monitoring and reporting services and use the provided information to revise standards and testing strategies based on real-world incidents.
R 4	Zenzic should maintain a directory of facilities available and their supported aspects of cyber-security testing.
R 5	A test facility should consider to facilitate testing classes of CAM beyond automobiles, such as UAVs, USVs and UUVs.

Future UK Position

The UK needs a sovereign capability in CAV cyber-security regardless of other countries' positions and should strive to be a leader in PNT system-of-systems resilience. Addressing the resilience of ITS system-of-systems is a hard challenge, but is also of high value in terms of national defence and UK export opportunities. Systems and facilities need to be resilient in the face of PNT attacks not just at the component level, but rather at the system-of-systems level. Whereas hardening against attacks risks a new attack finding a novel exploit path, resilience attempts to reduce the potential catastrophic impact of novel and unconsidered attacks. The adversaries that pose the highest threat, will combine and cascade attacks across systems to create an emergent effect at the system-of-systems level. Hence the UK needs to show leadership and focus on thorough secure and behind closed-doors testing, amongst other testing approaches, through supporting the PNT industry-leaders and independent expert research organisations.

Acknowledgements

This research was supported by Innovate UK [Grant No. 133896].

Project Team

- Dr Matthew Higgins (PI, University of Warwick)
- Prof Tim Watson (CoI, University of Warwick)
- Prof Paul Jennings (CoI, University of Warwick)
- Dr Matthew Bradbury (Researcher, University of Warwick)
- Dr Elijah Adegoke (Research-CoI, University of Warwick)
- Dr Erik Kampert (Research-CoI, University of Warwick)
- Jasmine Zidan (PhD student, University of Warwick)
- Steve Hickling (Spirent Communications Plc)
- Colin Ford (Spirent Communications Plc)
- Guy Buesnel (Spirent Communications Plc)
- Mark Hunter (Spirent Communications Plc)

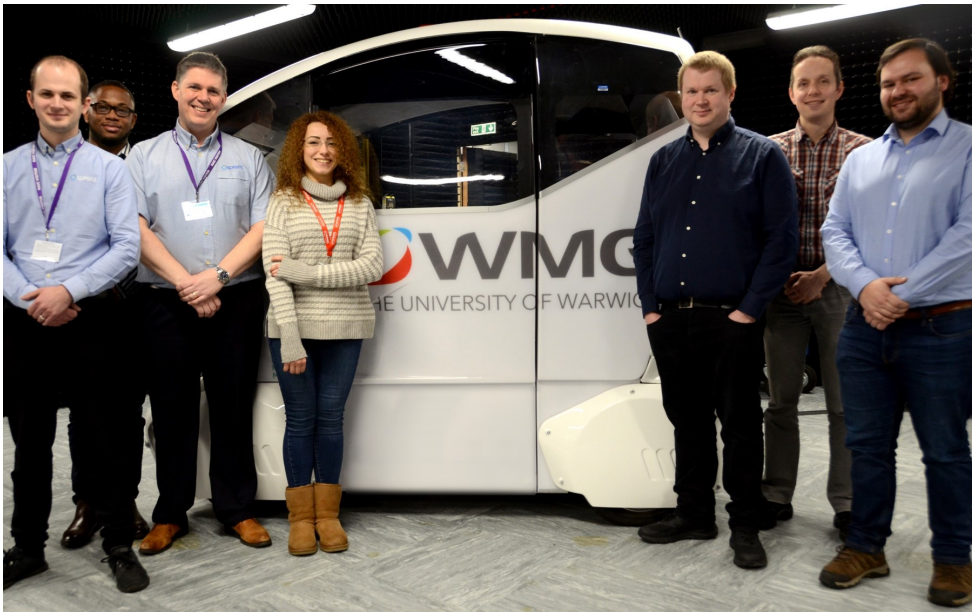


Figure 3: PNT Cyber Attack Resilience Project's Technical Team

Additional Acknowledgements

We would also like to thank the following colleagues for their assistance during this project:

- Dr Jakes Groenewald (CAM Testing Facilities Lead Engineer, University of Warwick)
- Harry Chan (VUT Safety Driver and Graduate Trainee Engineer, University of Warwick)
- Lee-Rose Jordan (Project Manager, University of Warwick)
- Daniel Martin (Spirent Communications Plc)
- Francesca Filippi (Spirent Communications Plc)
- Akis Drosinos (Spirent Communications Plc)

Project Team's Related Publications

- E. Adegoke, J. Zidan, E. Kampert, C. R. Ford, S. A. Birrell, and M. D. Higgins. Infrastructure Wi-Fi for connected autonomous vehicle positioning: A review of the state-of-the-art. *Vehicular Communications*, 20:100185, December 2019. ISSN 2214-2096. doi:10.1016/j.vehcom.2019.100185
- C. Maple, M. Bradbury, A. T. Le, and K. Ghirardello. A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis. *Applied Sciences*, 9(23):5101, November 2019. ISSN 2076-3417. doi:10.3390/app9235101
- J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, C. R. Ford, and M. D. Higgins. GNSS Vulnerabilities and Existing Solutions: A Review of the Literature. *IEEE Access*, pages 1–1, 2020. ISSN 2169-3536. doi:10.1109/ACCESS.2020.2973759

Most Relevant References

- C. Whitty and M. Walport. *Satellite-derived Time and Position: A Study of Critical Dependencies*. London, UK, 30th January 2018. URL `https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/676675/satellite-derived-time-and-position-blackett-review.pdf`
- M. Pattinson, S. Lee, Z. Bhuiyan, S. Thombre, V. Manikundalam, and S. Hill. Draft Standards for Receiver Testing Against Threats. Technical Report D4.2, STRIKE3, November 2017. URL `http://www.aic-aachen.org/strike3/downloads/STRIKE3_D42_Test_Standards_v2.0.pdf`. Issue 2.0

Contents

List of Tables **xi**

List of Figures **xi**

Abbreviations **xii**

1 Introduction **1**
1.1 Methodology . . . 1
1.2 GNSS Attacks Summary . . . 1
1.3 Related Recommendations . . . 2
1.3.1 STRIKE3 . . . 2
1.3.2 Government Office for Science Report . . . 3
1.3.3 Resilient Navigation and Timing Foundation . . . 3
1.4 Summary . . . 3

2 Community Experience **4**
2.1 Findings . . . 4
2.2 Summary . . . 6
2.3 Future . . . 7

3 Testing Experience **8**
3.1 Legality of Performing Tests . . . 8
3.2 Difficulties Associated with VUT Testing . . . 10
3.3 Impact Analysis of PNT Attack . . . 10
3.4 Conclusion . . . 11

4 Specifications and Recommendations **12**
4.1 Testing Preliminaries . . . 12
4.2 Testing Methodology . . . 13
4.3 Testing Environment . . . 14
4.3.1 Equipment Specification . . . 15
4.3.2 Test Environment: Anechoic Chamber . . . 16
4.3.3 Test Environment: Outside . . . 16
4.4 Metrics . . . 17
4.4.1 Vehicle Modes . . . 19
4.5 Test Cases . . . 19
4.5.1 Jamming . . . 20
4.5.2 Spoofing . . . 20
4.5.3 Software . . . 20
4.6 Controlled Testing . . . 20
4.7 Attack Feasibility Evaluation . . . 21
4.8 National Security . . . 21
4.9 Support System-of-Systems Testing . . . 22
4.10 Test Facility Employees . . . 22
4.11 Standards for GNSS Testing . . . 23
4.12 Subscribe to GNSS Threat Monitoring and Reporting . . . 24

4.13 Facility Directory 24
4.14 Non-Automotive Testing 25
4.15 Conclusion 25

5 Conclusions **26**
5.1 Findings 26
5.2 Specifications and Recommendations 27

Bibliography **28**

List of Tables

4.1 Black Box Testing Metrics [8] 18
4.2 Grey Box Testing Metrics [6, 7, 9] 18
4.3 Two Example Test Cases 19

List of Figures

1 PNT cyber resilience feasibility study carried out at Wellesbourne Campus . . . ii
2 Range of typical GNSS vulnerabilities iii
3 PNT Cyber Attack Resilience Project's Technical Team vii

3.1 Researchers preparing equipment for live, real-world tests at Wellesbourne Campus 8
3.2 VUT testing performed at Wellesbourne 9

4.1 Learning from a continuum of simulation, testing, trials and early deployment . . 13
4.2 Link Testing Continuum to V-process 14
4.3 Two examples of anechoic chambers for vehicular research 16
4.4 Reference Architecture showing vehicular system-of-systems [4] 22

Abbreviations

Notation	Description
BSI	British Standards Institution
CAM	Connected and Automated Mobility
CAV	Connected and Autonomous Vehicle
CNI	Critical National Infrastructure
ECS	European Committee for Standardization
ECU	Electronic Control Unit
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
ISM	Industrial, Scientific and Medical
ITS	Intelligent Transportation System
ITU	International Telecommunication Union
NMEA	National Marine Electronics Association
OEM	Original Equipment Manufacturer
OTA	Over The Air
PNT	Positioning, Navigation and Timing
PNTAE	Positioning, Navigation and Timing Attack Emulator
PPD	Personal Privacy Device
PPS	Pulse-per-second
RF	Radio Frequency
RMSE	Root Mean Square Error
RNP	Required Navigation Performance
SV	Satellite Vehicle
TTFF	Time To First Fix
TTPs	Tactics, Techniques and Procedures
UAV	Unmanned Air Vehicle
USV	Unmanned Surface Vehicle
UUV	Unmanned Underwater Vehicle
VSG	Vector Signal Generator
VUT	Vehicle Under Test
WI-FI	IEEE 802.11

1 Introduction

This report details experiences obtained performing cyber-security testing of the Positioning, Navigation and Timing (PNT) system on an example autonomous vehicle under test (VUT). Using this experience, plus lessons learnt from previous large-scale tests, and insight gained from interviews with experts, we present recommendations for cyber- and vehicle-testing facilities to support performing PNT cyber-security testing.

The remainder of this chapter will summarise attacks against GNSSs and also describe related projects that have previously made recommendations. A summary of the interviews performed with experts to understand the importance of testing and developing mitigations for these threats is presented in Chapter 2 and a summary of the practical testing performed in this project is described in Chapter 3. The specifications for a CAV-focused GNSS cyber-security testbed are presented in Chapter 4, including a number of advised recommendations. Finally, Chapter 5 summarises our findings, specifications and recommendations based on our survey of threats, interviews and testing, with the aim to improve the resilience of connected and automated mobility (CAM) solutions that require GNSS by cyber-security testing.

1.1 Methodology

In order to create specifications and recommendations for a GNSS cyber-security test facility for CAVs, with a specific focus on CAV PNT systems, we have followed below project methodology:

1. Survey literature in [2] to identify (i) threats, (ii) methods to detect threats, and (iii) techniques to mitigate these threats.
2. Ask relevant experts to provide input on which identified threats are high-priority and how a testbed should be designed to evaluate CAM system's resilience to these threats.
3. Perform a feasibility study by attacking GNSS receivers throughout the full test continuum, starting in the lab and finishing with live scenario tests, in order to understand how these testing environments complement each other, and to develop an optimised black box research methodology for the vast range of PNT attack scenarios.
4. Summarise this information and obtained experience to present recommendations for a new cyber test facility in this report.

This methodology led to the conclusion that PNT testing facilities are urgently needed across a wide spectrum of capabilities, from simulation in artificial environments to over-the-air testing in labs and real-world environments, and resulted in a set of specifications and recommendations for such facility.

1.2 GNSS Attacks Summary

This report focuses on three kinds of attacks on GNSS signals: jamming, spoofing and software. Attacking these signals does not require significant knowledge or expenditure in terms of resources, but can lead to significant impacts. This makes performing these attacks favourable to a threat actor, instead of performing more complicated attacks with greater resource and knowledge requirements.

Jamming is when an adversary denies access to position and timing information contained within a GNSS signal. It is the simplest PNT attack, as it requires an attacker broadcasting sufficient noise to prevent decoding of the GNSS signal, which is of low signal strength itself [10] compared to other common RF signals, such as Wi-Fi. Devices that perform jamming can be easily obtained for little money and operated without technical knowledge [11]. Users are typically aware that a jamming attack is occurring [12], but low-power jamming can be difficult to detect [13].

Spoofing is when an adversary supplies alternate GNSS signals containing position and timing information that may be different to that in the actual GNSS signals. Spoofing is harder to perform than jamming as the attack typically is performed stealthily with an aim to go undetected and slowly shift the position and time of the receiver. Performing a spoofing attack can be complicated, especially with mobile targets, due to the difficultly in making the produced signal appear authentic. Equipment to perform this attack is more expensive than equipment used to perform jamming, however, simple implementation can be obtained relatively cheaply [14].

Software attacks are an additional spoofing case to consider when maliciously crafted data is sent within the spoofed GNSS navigation message. As a GNSS receiver will need to decode and process the data within this message to calculate position, velocity and time, if there is a bug within this processing it could be exploited by crafted data in the message. One example in [15] spoofed the navigation message such that a satellite was located at the centre of the Earth. This led to a denial of service attack against the GNSS receiver, because it caused a division by zero error that was repeated each time the receiver restarted as it had cached the malicious value.

1.3 Related Recommendations

There has been a great deal of interest in securing GNSS for a variety of systems in the past. This includes interest from GNSS maintainers, academia, industry, and government. In this section, projects and groups that have previously made recommendations about the cyber-security of GNSSs will be summarised. Recommendations made in those projects will be used to inform the recommendations that are made in this report.

1.3.1 STRIKE3

The STRIKE3 project, which ran from February 2016 to January 2019, aimed to produce a non-sector-specific, standardisation of GNSS threat reporting and receiver testing [16, 17]. Multiple sensors were installed to detect potential GNSS attack events. The STRIKE3 project focused its efforts on GNSS jamming due to the ease and likelihood of such an attack being performed. The researchers in STRIKE3 discounted spoofing and meaconing [7, § 2.4.1] due to the anticipated difficulty, equipment requirement and desire to focus testing the impact of interference observed in real-world monitoring. However, events such as [18, 19] mean there are intentional and unintentional spoofing attacks that need to be considered when testing GNSS receivers.

As part of its data gathering on jamming events, the STRIKE3 project built a database of GNSS jamming attacks [20] which was grouped into 11 broad attack classifications. This information was used to draft standards for threat monitoring and reporting [12, 21] and testing of GNSS receivers [7]. We recognise that those standards for GNSS jamming are comprehensive and will form the basis of our recommendations for testing GNSS jamming. As these recommendations target the behaviour and functioning of CAVs, there will be some differences due to the higher system level focus. We are also of the opinion, that it is important to consider spoofing and other classes of attacks that are not considered in STRIKE3, therefore, we will make additional recommendations for those other kinds of threats.

1.3.2 Government Office for Science Report

In 2018 the UK's Government Office for Science produced a report [6] on GNSSs, threats and the potential impact attacks could have across the UK's critical national infrastructure (CNI). As part of this report, Chapter 5 discusses standards and testing of systems using GNSS to supply PNT information. Whereas a number of standardisation initiatives were highlighted, the report concludes that there is still a need for a unified standardisation approach. This includes specifying a single set of metrics to assess systems against. In terms of testing, the report highlights three main issues: (i) there are no common testing standards, (ii) testing a system-of-systems is difficult, and (iii) there is a lack of information about what UK-facilities are available to perform tests at. These are also issues that need to be addressed for the testing of PNT attacks against CAM systems.

1.3.3 Resilient Navigation and Timing Foundation

The Resilient Navigation and Timing Foundation have published a number of US-focused recommendations for GNSS resilience [22]. These recommendations fall under three categories: protect, toughen and augment.

Protect describes recommendations to locate jamming (similar to STRIKE3), improve legislation, and prevent transmissions in adjacent frequency bands from exceeding the power limits.

Toughen describes using GNSS receivers with jamming and spoofing-resistant technology, using more than one PNT source for CNI, and having CNIs continuing normal operations when GNSS service is disrupted.

Augment describes using alternate PNT sources other than GNSS to augment localisation and time synchronisation of a system.

These recommendations are useful high-level guidelines for industry and government to follow. Testing facilities should aim to evaluate the level of resilience that systems which followed these guidelines have obtained.

1.4 Summary

Whereas previous work exists, that made recommendations about testing the resilience of GNSS to provide PNT in general, there has been a lack of work that focuses on its vehicular context. This report will make recommendations that are focused on the specific requirements of vehicular-focused testing. Some of these recommendations overlap with general PNT testing, however, others arise due to the design of connected and autonomous mobility systems.

2 Community Experience

In order to understand which of our identified threats are currently being performed, are believed to have a high impact and where future effort needs to be focused, we interviewed a range of experts with experience and knowledge of GNSS attacks and automotive cyber-security. This chapter will present a summary of the results from these interviews, highlight important issues and future areas for investigation that were raised by the experts being interviewed. Interviews were separately performed by Spirent and WMG. The interviews performed by WMG were granted ethical approval to be performed by the University of Warwick's Biomedical & Scientific Research Ethics Committee [BSREC 61/19-20].

2.1 Findings

GNSS Importance and Threats

> "GNSS provides extremely low cost, accurate time, and position and velocity data."

> "The time aspect is always important, location depends on where the vehicle ends up being — a fall back must exist — e.g., in an area where positioning signals are difficult to receive, they cannot just hand back control directly to the driver."

> "The threat is very real — we have gathered over 100 records of incidents/attacks, which were a mix of deliberate and accidental incidents, covering all areas from accidental leakage, to malfunctioning devices and fraud."

The importance of GNSS to supply PNT information was highlighted by the interviewees. This includes both the position and timing information included in the GNSS signal. Some participants had experienced attacks being performed, whereas others were aware of databases (e.g., STRIKE3) that recorded real events.

Adversaries

> "The objective of the attacker needs to be determined before evaluating the severity. The mindset of the adversary is essential to determine the severity of effects. All could be low or high impact. Objectives can vary widely."

Our interviews failed to conclusively identify if jamming or spoofing were higher priority threats to focus on. Jamming can be easily performed, easily detected and can be difficult to mitigate, whereas spoofing is often harder to detect, harder to perform, but can cause greater impacts. One conclusion was that it is important to evaluate adversaries and their capabilities in combination with the context in which vehicles will be attacked in order to be able to identify threats and evaluate their impact.

> "Many receivers we tested had anti-spoof technology, but could still be spoofed."

> "There will be a growth in use of SDR technology to attack CAVs due to its high availability and low-cost SDRs are already being used for a variety of RF cyber-attacks e.g., in car thefts based on keyless systems."

The technology used to perform these attacks is becoming more sophisticated, more available and at a lower cost. Technologies such as SDRs may increase the likelihood of being impacted by jamming and spoofing threats due to lower barriers to entry for adversaries.

Mitigations

> Safety and security need to be investigated hand-in-hand.

> CAV is part of an ITS. So security of the rest of the ITS needs to be studied. A CAV can also be an attack vector to an ITS and this also needs to be studied. The security of a CAV cannot be addressed in isolation.

There is a need for security to not be considered in isolation. It is vital that safety and operational aspects of a vehicle are also considered when providing security. This is difficult due to the complexity of the system in which a CAV operates. Testing facilities need to provide suitable space to ensure security mechanisms do not impact safety and include ways to test how quickly a CAV can recover from attack. As these attacks may be persistent, some permanent facilities are required to perform long-term testing. Testing facilities will also need to provide infrastructure on which attacks can be emulated, so the impact on a CAV can be examined.

Fusion With Other PNT Sources

> I would like to see other signals/alternative technologies to aid and support navigation which would improve resilience over time.

> Improve robustness and resilience by having an alternative positioning system. Vehicles already have IMU and other sensors to cover the position when GNSS signal is lost, and then they use mapping software which results in a good quality level of the position. But for fully autonomous vehicles, accuracy is more important, so a higher level of robustness to spoofing is required.

One key point regarding the resilience of a PNT system is the need to fuse information with alternate sensors. As a vehicle will not only have access to GNSS to provide PNT information, the other sensors such as IMUs, LIDAR, and local clocks need to be used to provide redundancy when GNSS is under attack and vice versa. However, this raises further considerations as the weight of trust between sensors needs to evaluated. Future testbeds need to be able to support verifying the ability of these sensors to provide redundancy and also be able to test concurrent attacks against multiple sensors.

Facilities

> A test facility is key, both a real-world and synthetic capability (such as a digital twin) to create conditions that represent an attack that might be used on a system.

> Access to a national database of testing facilities would be useful due to the difficulties of performing practical testing without a Faraday cage.

The need for either more testing facilities, or an increase in their discoverability was highlighted by the participants. There is a need for facilities with a wide range of testing capabilities for CAM systems (such as for shipping and drones) and not solely for CAV systems. These facilities need to support a spectrum of testing from simulation to real-world OTA testing. The other aspect that was highlighted was the need to include environmental considerations both when performing testing with simulators, and when performing OTA testing in anechoic chambers. This is necessary to improve the real-world relevance of this testing.

Testing

> Consider architectures of different vehicle manufactures of different PNT implementations and architectures. Different architectures would be hacked different ways. Testing needs to be manufacturer agnostic and should be able to apply to different manufacturer architecture.

When performing testing it is important to not solely focus on the impact of the vehicle, but also consider indirect impacts from attacks on infrastructure and other interacting systems. This testing needs to be designed in a generic way to facilitate testing arbitrary combinations of equipment from different OEMs. Test facilities will also need to be able to undertake testing from a wide system-of-systems perspective, which will include testing additional equipment that is connected to or interacts with a vehicle.

Personnel

> It is not only about investing in the technology and the infrastructure, but also about the people and the process. Therefore, you need to have the technology in place and then you need to train the people how to use the technology and understand the differences in the technologies applied. You also want to train people in matters of raising awareness on what they are doing and what problems could appear, so they can report any abnormality that they identify.

While technology can be key in detecting and mitigating attacks on GNSS systems, it is important to consider the human element of securing a complex system. While mandating a human-in-the-loop for all autonomous activities may be undesirable, it may be suitable for highly trained staff to monitor events at a higher level. Such staff would need to apply suitable training and intuition to identify attacks that autonomous systems may not be looking for.

2.2 Summary

The opinions provided by the experts interviewed highlighted that jamming, spoofing and timing attacks are all practical for an attacker to perform and can lead to impacts on a vehicle. We have made some general conclusions in areas where general (if not unanimous) agreement was observed by participants in the survey. However, the conclusions expressed below do not necessarily reflect the views of all of the individual participants or of the organisations they represent. The conclusions drawn from these interviews have been used to inform the specifications required for GNSS cyber-security CAV test facilities and also the recommendations that have been made in Chapter 4.

- The threats to CAV PNT cyber-security should be dealt with as a high priority matter.
- There is a need to develop a common and consistent methodology for assessing PNT cyber-security risks.
- There is a need to consider the impact of sensor fusion on testing attacks and developing mitigations.
- The responsible disclosure of incidents and discovered vulnerabilities is essential in the commercial sector, especially for safety and liability-critical applications such as CAV.
- There is a risk that manufacturers expect a certain level of performance from the devices they procure, hence do not test them for resilience and robustness themselves.

2.3 Future

From these interviews, other than the valuable input into the state of the threat landscape and testbed specifications, there are three sets of collaborations that the CAV-focused field would benefit from having future engagements with.

1. The newly announced National Timing Centre in the UK has the aim to improve "security and resilience, communication and implementation of new technologies, and pave the way for trusted time and frequency across the country" [23]. The UK CAV industry may find it advantageous to work with the National Timing Centre to develop new methods for delivering and securing the precise timing data needed by CAVs.

2. There is room for greater co-ordination/co-operation between agencies and industry. The STRIKE3 project [12] has shown that the collection, storage and characterisation of real world interference threats is possible, but the sharing and reporting mechanisms are currently fragmented and un-coordinated.

3. The range of opinions given by all survey participants suggests that a future public round table involving CAV cyber-security stakeholders from industry, government, academia, regulators and institutes could prove to be very beneficial to all parties involved in CAV PNT system cyber-security.

3 Testing Experience

This project has shown that the chosen Lab2Live methodological approach, starting with lab-based testing on isolated GNSS-receivers and finishing with real-world tests on a black box CAV, provides the complimentary and comprehensive results that are required to evaluate a system's PNT cyber resilience [2]. In the laboratory, controlled tests were carried out on three GNSS receivers using Spirent's PNT attack emulator (PNTAE) for spoofing attacks and a vector signal generator (VSG) for replicating intentional electromagnetic interference. In the lab-based tests, observable parameters such as the signal power, number of visible satellite vehicles (SVs), and the time-to-first-fix (TTFF) of the respective receivers were evaluated with respect to emulated jamming and spoofing attacks. This fed into the development of model-independent, black box research methodologies for real-world, live-sky tests, as would be used in a cyber-physical testing facility when certain detailed component-level information might neither be disclosed nor otherwise available. In Figure 3.1, the attack emulators for the respective tests are shown, and Figure 3.2 displays the VUT and its trajectory at the Wellesbourne Campus of the University of Warwick. Generalising the live results, leads to the conclusion that real-world testing on a CAV-system can result in distinctively different observations than those made in a lab environment. This can be understood through the influence of the GNSS implementation in the CAV's operating system and potential sensor fusion algorithms, e.g. including the inertial navigation system (INS); cameras and radar, on the associated decision-making processes. As these results complement each other, in order to determine a CAV's or CAM PNT cyber resilience, tests should thus be carried out that span the full continuum, from simulation to emulation, to tests on intelligent vehicles inside a dedicated lab, to real-world environment testing on autonomously-driving vehicles.

(a) Mobile jamming set-up

(b) Mobile spoofing set-up

Figure 3.1: Researchers preparing equipment for live, real-world tests at Wellesbourne Campus

3.1 Legality of Performing Tests

In the UK there are two main pieces of legislation that need to be considered when performing the type of tests (jamming and spoofing of GNSS signals) envisaged in this feasibility study. The first and most important is Section 68 of The Wireless Telegraphy Act 2006, which deems

(a) VUT at Wellesbourne

(b) VUT test trajectory

Figure 3.2: VUT testing performed at Wellesbourne

jamming and spoofing of signals illegal in the UK. For this study, therefore, we have either performed indoor OTA tests inside an anechoic chamber, or outdoor non-OTA tests during which the jamming or spoofing signal was added to the authentic signal through coaxial cables and a high-power RF combiner, with negligible spurious emissions. The second piece of legislation is The Electromagnetic Compatibility Regulations 2016, SI 2016/1091 which restricts the import and sale of jammers and requires that apparatuses must not cause excessive interference. The attack emulators used in this feasibility study are test signal generators and their transmissions are strictly contained either over coaxial cable or within an environment that do not allow for RF leakage, such as an anechoic chamber or a Faraday cage.

Currently, the regulator for the UK communications services (Ofcom) only allows GNSS jamming testing by the Ministry of Defence, and considers it a crime if carried out by anyone else [24, § 68]. To use any radio transmitting device in the UK, it will need to either be licensed, or have a specific licence exemption. Ofcom's most related licence products are the GNSS repeater licence and the Innovation and trial license[1]. The latter is a non-operational licence for testing, research or demonstration, and is also recommended for work carried out inside a Faraday-shielded chamber. The detailed information regarding these pieces of legislation should be fed into LR43 [26, p. 99] on the Zenzic Roadmap, and used to simplify the process of obtaining relevant licences to perform testing, or to document under which circumstances these licences are not required.

An alternate approach to mitigating these legal issues is to up or downconvert GNSS frequencies before transmission and after reception. In [8], GNSS frequencies were downconverted from 1575.42 MHz to 915 MHz in the US ISM band, and vice versa. The ISM bands are for industrial, scientific and medical applications, and other applications using them (e.g. telecommunication) must tolerate any interference generated from ISM applications. A downside to this technique is that the down-conversion could change aspects of the signal which may lead to attacks and defences not precisely matching those that an attacker would use to attack the system and/or the techniques the system could use to defend against those attacks. More research is needed to determine the efficacy of such testing approach.

[1] `https://www.ofcom.org.uk/manage-your-licence/radiocommunication-licences/non-operational-licences`

3.2 Difficulties Associated with VUT Testing

Locating and Interfacing with GNSS receiver

Depending on how much technical detail a mobility OEM can share about the PNT receiver system and its peripheral sensors (e.g., antennas locations), access to the individual components allows systematic testing at all relevant scales and complexities of the test continuum. This also includes taking into account the potential differential GNSS implementation in the receiver.

Interfacing with ECUs

Depending on the level of embedding of the GNSS receiver, and possible fusion processes with other automotive sensors, access to the relevant electronic control units (ECUs) is crucial for an in-depth understanding of the attack's impact.

Sensor Fusion

In a black box CAV testing scenario, it is difficult to pinpoint the influence of potential sensor fusion algorithms, e.g., including the INS; cameras and radar, on the associated decision-making processes.

Lab versus Real-World

As highlighted in [2], results from lab-based and real-world PNT testing can differ substantially. A set of comparable metrics and a robust research methodology should guarantee that the results are complementary to each other. Furthermore, adapting a CAV to real-world, spurious emission-free OTA attacks using a custom enclosure for its GNSS receiver and the attack antenna, requires innovatory engineering steps to guarantee reliability during mobile testing.

Health and Safety

Real world attacks on CAVs can trigger unexpected behaviour. Adequate precautions thus have to be taken, e.g. to facilitate movement outside the expected trajectory, but also to stop the VUT when a PNT attack is in progress.

Power Supply

During real-world, mobile, field tests, testing equipment requires a safe and reliable power source. As commercial power inverters in-between a potential electric-powered CAV's battery and the equipment might not support the required power levels, uninterruptible power supplies could be best suitable.

3.3 Impact Analysis of PNT Attack

Black box, grey box and component-level testing each allow for different depths in their analysis of the impact of a PNT attack. Whereas for the latter all essential PNT parameters of interest can be observed and possibly recorded, for the former two, if no GNSS telemetry output is available (e.g., in NMEA format) sometimes the impact of the attack can only be derived from the CAV's behaviour. In particular, it is difficult to:

- know whether the autonomous vehicle uses PNT information provided by GNSS.
- know which GNSS constellations are implemented in the GNSS receiver.

- know when sensor fusion is implemented, how that sensor information interacts with GNSS inconsistencies?
- test the impact of timing attacks.

Under these circumstances, it is best to start with the most basic jamming and spoofing attacks, followed by slowly increasing realism, depending on the kinds of attacks that can be simulated with the GNSS testing equipment, as described in [2].

- Start with most basic and only include the spoofed signal
- Increase realism by including both the real signal and the spoofed signal

3.4 Conclusion

Lab-based device and CAV PNT cyber testing allows for a controlled and partially programmable research methodology, with straightforward to reproduce results. Live testing, on the other hand, involves a number of uncontrollable and unknown parameters which increase the amount of required testing before a well-founded conclusion can be made about a VUT's PNT attack resilience. Real-world CAV and PNT testing is bounded by legal restrictions, amongst others on spurious RF emissions. Real OTA PNT attacks to a VUT, mimicking most realistically an adversary's capabilities, are thus difficult to achieve without a dedicated, limited-access, large area, testing facility.

4 Specifications and Recommendations

Based on a survey of related academic literature, our experiences performing practical testing, and the knowledge gained by interviewing experts in the community, in this chapter we present recommendations on the specifications for a CAV cyber-security test facility and other relevant recommendations.

4.1 Testing Preliminaries

Before performing testing it is necessary to understand the context within which systems will be used and put under threat of attack. This context should then be used to guide how cyber-security testing of the system is performed.

1. Identify who the threat actors are, what goals, motivations, resources, knowledge and presence they will have. Use this information to inform the kinds of testing that will be performed.
    - Goals: What is the threat actor trying to achieve?
    - Motivations: Why does an adversary want to perform a GNSS attack?
    - Resources: What equipment/tools/finance/personnel/etc does the threat actor have?
    - Knowledge: What information does the adversary have? How does this impact the way in which they perform GNSS attacks?
    - Tactics, Techniques, and Procedures (TTPs): Is the attack likely to be slow and silent, requiring persistence on the system, or quick and noisy? How will attacks likely be conducted?
2. Build representative test cases for the identified threats that may be executed.
3. Perform safety and risk assessment for test cases.

Although difficult, it is useful to identify the risk posed by threats and use the calculated risk level to prioritise implementing mitigations for threats. Risk is typically calculated as the impact of a threat (e.g., financial cost) multiplied by the likelihood of the threat (a probability). An example of this risk calculation was performed by the Resilient Navigation and Timing Foundation in [27], where the highest impact was calculated for jamming attacks performed by criminal, terrorist, and military-level threat actors.

As per TD09 in the Zenzic Roadmap [26, p. 97], a national threat database needs to be created. Information on threat actors should be included in this database in order to contextualise the threats in that database.

Specification 1: A set of standard threat actors who attack GNSS systems should be defined, e.g., by the National Cyber Security Centre, and made available to the testing facility. Tests should then focus on these threat actors. This list should be revised over time as the threat landscape evolves.

4.2 Testing Methodology

When designing tests for arbitrary CAM solutions there may be limited access to internal aspects of the system. In this case the system needs to be treated as a black box. However, if greater access to the internal systems is available then grey box testing can be performed. Grey box testing allows for a more targeted approach due to knowledge of the system. It is also important to understand how much access to the vehicle's telemetry is available. Additional metrics can be evaluated for a test case when the testers have access to detailed telemetry from the vehicle.

1. Treat the autonomous vehicle as a black box, without access to telemetry:
    - Identify scenarios in which to perform testing.
    - Perform control experiments (VUT not under attack) to obtain baseline performance.
    - Observe VUT behaviour and evaluate if deviations occur when comparing control experiment to simulated GNSS attack.
    - Evaluate if deviations are expected or not.
    - Use a secondary GNSS receiver which receives the same input as the vehicle's receiver to verify that the GNSS testing equipment has the intended impact.
2. Treat the autonomous vehicle as a black-box, with access to telemetry:
    - Perform the same testing as for Level 1.
    - Use VUT telemetry information to verify that GNSS testing equipment has the intended impact.
3. Perform grey box testing on the autonomous vehicle:
    - Perform the same testing as for Level 2.
    - Use knowledge of internal structure of the autonomous system to identify specific tests that target internal systems.
    - Use these tests to evaluate the impact of GNSS attacks on these internal systems.

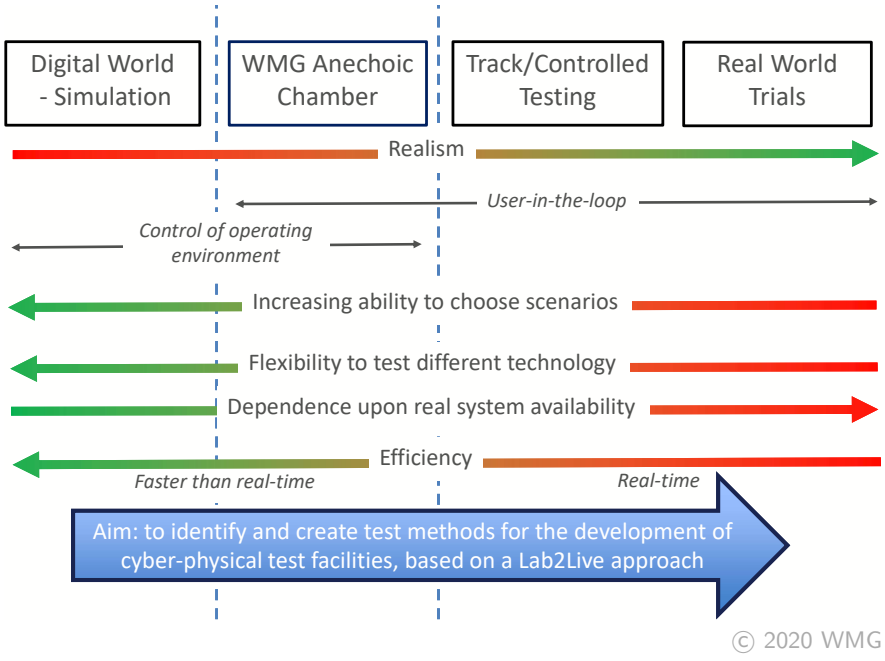


Figure 4.1: Learning from a continuum of simulation, testing, trials and early deployment

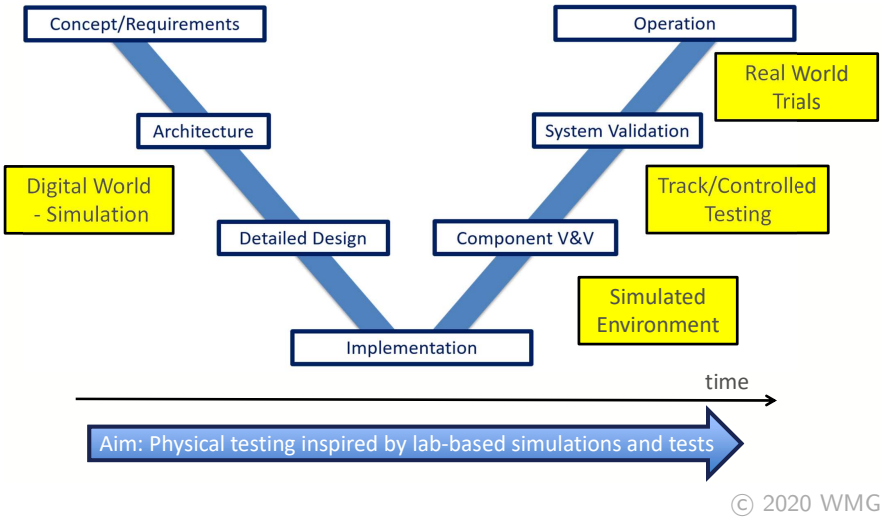


Figure 4.2: Link Testing Continuum to V-process

4.3 Testing Environment

The practical feasibility study that has been carried out in the course of this project follows WMG's Intelligent Vehicles research team's view on achieving CAV adoption through the learning from a continuum of simulation, testing, trials, and early deployment. It is important that testbeds are able to facilitate cyber-security testing across such continuum with a Lab2Live approach, as shown in Figure 4.1, starting with computer-based simulations that provide a first input on parameters and their ranges of interest, as well as hard- and software requirements for physical experiments on the device or vehicle of interest. Lab-based work in a closed environment then supports the control of most external parameters, allowing for high reproducibility and potential programmable repeatability of tests. Moreover, a lab provides a safe environment in which controlled scenarios can be investigated, in particular the corner-case scenarios that are unpractical or impossible to carry out in the real-world. Finally, live tests and measurements are required for guaranteeing a device's level of operation under real-world conditions, whilst experiencing real noise and interference for all sensors that interact with the device and might be affected by them. This allows the resilience of a VUT to first be evaluated in a highly controlled environment and then move to a less controlled, but more realistic, environment, as graphically depicted in Figure 4.2.

Specification 2: A test facility should support performing tests over the full range of the test continuum, from simulation to emulation to testing in a real world environment.

There need to be sufficient capabilities across the UK to support the testing of jamming or spoofing GNSS signals: (i) using GNSS testing equipment via a physical connection to the CAV's GNSS receiver or (ii) an over-the-air attack with a portable GNSS simulator enclosed within a anechoic chamber.

If possible, specific test sites should also aim to (iii) support live, outdoor, jamming or spoofing of GNSS signals. This is required to test the feasibility of such attacks in a real-world environment and to further improve the simulations of such attacks.

4.3.1 Equipment Specification

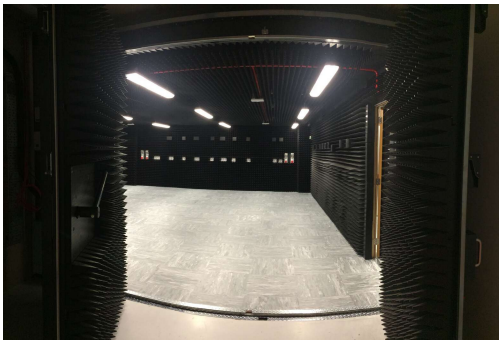
In order to perform testing of GNSS receivers, attack emulators will need to support specifications similar to those listed below.

- Multiple constellations:
  - GPS and Galileo as baseline options. Simulator should support GLONASS, Beidou and QZSS to ensure generic appeal and to fully exercise devices that support these constellations.
    - 16+ channels available per Code simulated.
      - Ensure all SVs in sight can be modelled.
      - Ability to transmit PRN code without Nav Data.
    - Required for achieving Nav Data spoofing.
- Rinex ephemeris data:
  - All Rinex parameters must be simulated in order to match live sky (including SV clock and system offsets).
- Realtime operation:
  - No pre-processing required so spoofing attacks can be easily performed.
- Signal Accuracy:
  - Pseudorange Accuracy 3 mm RMS
  - Pseudorange Bias 0 mm RMS
  - 1PPS to RF Alignment $< \pm 2$ ns
  - Inter Frequency Alignment $< \pm 250$ ps (± 75 mm)
- Simulator interfaces:
  - -60 dBm (High power) GNSS output
    - This is to ensure that there is sufficient GNSS signal strength to attack the CAV's GNSS antenna directly.
  - 1PPS input
    - To synchronise the simulator's 1PPS event to GPS 1 s epoch (from Reference receiver). (< 50 ns).
  - 10 MHz input
    - To ensure drift between simulator and live sky is controlled.
- Other features:
  - Hardware iteration rate of 100 Hz.
  - Realtime remote 6 degrees of freedom trajectory control — Low motion latency less than 40 ms, measured from point of remote motion input of external sourced vehicle dynamics to simulation at RF output.

Specification 3: The equipment used to perform PNT attack emulation should support technical capabilities that are necessary to perform testing.

Other equipment will also be needed for a testbed, such as portable battery power supplies to power the PNTAE equipment during mobile test scenarios, and equipment to ensure the safety of researchers inside and outside of vehicle, as mentioned in Section 3.2.

4.3.2 Test Environment: Anechoic Chamber



(a) Vehicle entrance to WMG's anechoic chamber inside the National Automotive Innovation Centre

(b) Vehicle under test in WMG's anechoic 3xD Simulator inside the International Manufacturing Centre

Figure 4.3: Two examples of anechoic chambers for vehicular research

Due to the legal requirement to ensure that jamming and spoofing resilience testing does not have an impact on valid users of GNSS services, it is vital that access to an anechoic chamber is provided at a testbed. This allows the facility to ensure that any hardwired equipment does not leak excessive interference and also allows performing OTA testing on the target. At minimum these chambers should be sufficiently large to support multiple personnel testing individual receivers, preferably the chamber should be sufficiently large to support bringing a vehicle in to perform testing on. An ideal chamber would be large enough to support simultaneous testing of multiple vehicles.

Specification 4: A test facility should provide access to an anechoic chamber to allow legal testing of OTA attacks on GNSS systems.

4.3.3 Test Environment: Outside

As well as an internal and enclosed chamber, it is vital that testbeds have external facilities which the resilience of a CAV to GNSS attacks can be tested in. This is necessary because an outside testing space will provide more realistic conditions (compared to inside a chamber), allowing testing to be performed that is more representative of the environment in which vehicles

may be attacked. It is necessary for a test facility to provide access to multiple environments, as the kinds of attacks and how they are performed may be impacted by the environment in which the vehicle and adversary are operating in. Due to legal reasons this testing will likely require non-OTA testing, where a malicious signal is supplied by a physical cable instead of being wirelessly transmitted.

Specification 5: A test facility should provide areas in which non-OTA testing can be safely performed in real-world environments. A variety of environments (e.g., urban, rural, motorway) need to be supported to test the environmental impact on an attacker's capabilities and the impact on the implemented mitigations.

4.4 Metrics

In order to evaluate the attack resilience of a system, first a set of metrics needs to be defined. These metrics have been split into two categories, for when a black or grey box approach to testing is used. With respect to the performance of the GNSS receiver and/or the CAV, the following criteria which have been adopted from the required navigation performance (RNP) concept and aspects of the CCAV code of practice [28]:

Accuracy characterises the localisation error between the ground truth and the estimated position of the CAV. The root mean square error (RMSE) is widely used in the academic literature and can be obtained using Equation (4.1), where x_i and y_i are the estimated coordinates/position and x, y are the ground truth coordinates. The maximum absolute position error, mean absolute position error or euclidean error can also be adopted [3, 5].

$$\mathrm{E}_{rmse} = \sqrt{(x - x_i)^2 + (y - y_i)^2} \tag{4.1}$$

Integrity characterises the correctness of the information supplied by the PNT system. Furthermore, integrity measures the ability of a navigation system to provide the user with timely warnings when the information provided is inaccurate. The integrity of a navigation system can be reported via the alert limit, integrity risk, time to alert and protection level [29].

Continuity measures the ability of a GNSS/PNT receiver to operate without failure or interruption. In the academic literature and industry, it is usually referred to as a probability that the receiver is operational after initialisation. It is directly related to integrity and accuracy, hence it describes the probability of having a reliable operation over a specified period [29].

Availability is the amount of time a GNSS/PNT receiver provides usable PNT information. It generally represented as the percentage of time in which the navigation system is usable. In regards to CAVs, GNSS availability can be defined as the percentage of the measurement epochs where the terminal delivers the considered output with the required performance irrespective of signal strength [30].

Resilience measures the ability of a system to recover after being attacked. An aspect of resilience is the length of time the system takes to recover. During this recovery period, it is important to consider what functionality is available during this period.

Safety properties ensure that the system does not enter into a state which would place the vehicle or its occupants in danger. This property may be evaluated in terms of risk, where safety is defined as the absence of unavoidable risk [28, §2.7].

Specification 6: A standard set of metrics needs to be defined and used to evaluate the resilience of CAM systems when their PNT system is under cyber-attack.

A key component of defining these types of metrics is that for each one a performance measure needs to be provided. During performing testing, the response of the VUT needs to be within this tolerance. For example, if a VUT's GNSS receiver is jammed, the expected outcome could be that the vehicle comes to a stop, and the performance measure could be the time taken for the vehicle to come to that stop. This value will be based on various scenario-related aspects, such as the vehicle, the adversary's jamming approach, the jamming equipment used, and the road environment. Therefore, future work needs to consider what performance measures should be set to test vehicles against. Section 5 of [31] presents security performance metrics which could form a useful starting point for the definition of these performance measures.

Table 4.1: Black Box Testing Metrics [8]

#	Description	Performance criteria
BB1	Vehicle Stops	Safety
BB2	Vehicle continues moving along desired route	Availability
BB3	Vehicle recovers after attack	Resilience
BB4	Vehicle requires human intervention	Resilience

Table 4.2: Grey Box Testing Metrics [6, 7, 9]

#	Description	Performance criteria
GB1	GNSS receiver continues to generate NMEA messages	Availability
GB2	Position Accuracy	Accuracy
GB3	Number of visible SVs	
GB4	Number of SVs used	
GB5	Time to first fix (s)	Availability
GB6	Timing error (ns)	Accuracy
GB7	Re-acquisition time	Availability
GB8	Ability to switch between PNT sources	Continuity

4.4.1 Vehicle Modes

Vehicles (and especially autonomous vehicles) may operate in different modes, where only certain kinds of sensor input are used to perform autonomous tasks. If a vehicle supports operating in a GNSS-only mode, it is important to test both that mode and other modes which fuse GNSS with other sensor input. This allows the resilience to GNSS attack to be evaluated when other sensors are available.

Recommendation 1: Vehicles should be tested in various driving modes (if possible): (i) GNSS-only and (ii) fusion of GNSS with other vehicle on-board sensors.

As highlighted by the interviews performed, vehicles will use a wide array of sensors to obtain PNT information. An adversary will potentially attack these sensors individually, the GNSS receivers individually, or a combination of sensors (such as LIDAR and IMU). Testbeds need to be able to support performing testing on combinations of attacks against multiple sensors.

Specification 7: A test facility needs to be able to support evaluating the resilience of a vehicle against single and multi-sensor attacks.

4.5 Test Cases

TD11 in the Zenzic Roadmap [26, p. 97] specified that a set of scenarios needs to be designed that will be used to perform reproducible cyber-security testing.

Specification 8: A standard test suite of GNSS jamming and spoofing attacks should be defined and made available to organisations performing testing at different test facilities.

Table 4.3: Two Example Test Cases

Name	Description	Attack Aim	Black Box	Grey Box
Straight Line Jamming	Adversary jams GNSS signals while the vehicle is travelling in a straight line (varying techniques available).	Prevent vehicle from having access to position or timing information	BB1 / BB2	GB1–9
Spoofed GNSS Variables	Adversary spoofs the GNSS data stream to include invalid values.	Prevent GNSS receiver from correctly calculating position or time	BB1 / BB2	GB1–9

4.5.1 Jamming

While jamming tests using GNSS simulators are fairly understood, extensive tests also need to be carried out with jammers such as personal privacy devices (PPDs) as seen in unintentional jamming attacks. The electromagnetic features of these devices are known to vary widely. Jamming detection and mitigation techniques can then be evaluated and characterised with respect to decoupled PPDs; whereby a diverse range of PPDs are disassembled and the RF components parameterised in a controlled RF enclosure such as a Faraday cage.

4.5.2 Spoofing

Given that different vehicle manufacturers will use different GNSS receivers and implement different integration and operating systems, extensive field tests need to be carried out using spoofing simulators/emulators (such as Spirent's PNTAE) in the field. By using a simulator/emulator designed to specification, representative, repeatable, affordable and controlled tests can be carried out in the field. Testbeds with such features would provide avenues for CAM system and service designers to evaluate heterogeneous implementation architectures adopted by vehicle manufacturers. Furthermore, by carrying out field tests using spoofing emulators/simulators, the behaviour (safety and availability) of CAVs can be isolated from that of the GNSS receiver when subjected to a series of spoofing attacks.

4.5.3 Software

The primary test case for GNSS software attacks will be to spoof a signal with specific values for high impact variables in the navigation message data included in a GNSS signal. For GPS this will include: (i) Ω_0: the longitude of the ascending node of the orbit plane at weekly epoch, (ii) $\dot{\Omega}$: the rate of right ascension, and (iii) $\sqrt{A}$: the square root of the semi-major axis [15, 32]. Due to the large state space and long time period to receive this information, only a limited number of values can be tested. Specific values should be chosen (such as $0 = \sqrt{A}$) based on the potential for a high impact, to be tested together with a small number of random values.

4.6 Controlled Testing

In order to perform effective testing, it is necessary to compare the effects of testing on an unknown vehicle to a control vehicle that has already been extensively tested. This ensures that when tests are performed, there is greater confidence in the test when the control vehicle's response is the expected response. This facilitates accounting for variables in a test that may be difficult to keep similar when testing in a real-world environment.

Specification 9: A test facility should supply a group of control vehicles with known functionality and responses to a test suite. This is in order to:

- Ensure the test has the same impact on the control vehicle.
- Evaluate the possible different impacts on the test and control vehicle.

4.7 Attack Feasibility Evaluation

PNT attack emulators are capable of perfectly emulating GNSS signal attacks. It is important to perform PNTAE-based testing in a real-world environment in order to determine the feasibility of an adversary performing such an attack, albeit of a lesser quality. For example, OTA PNT attacks on a moving CAV are the most difficult to perform, because of the difficulty anticipating the vehicle's trajectory in order to accurately determine its relative motion to the attacker. A possible testing solution is a mobile PNTAE that can be positioned and operated from inside the CAV, and coupled to the CAV's GNSS receiver through an external antenna.

Specification 10: A set of appropriate sites need to be identified where PNT attacks can be performed in real-world environments in order to understand and demonstrate the feasibility of an adversary performing these attacks.

4.8 National Security

Testbeds that undertake cyber-security testing need to consider the relation of the testing to national security. Firstly, the testing needs to be performed such that pertinent threats to national security are focused on. This means that a testbed needs to have a connection to receive up-to-date information from the defence sector. Secondly, as testing could be performed on systems that either interact with or form part of the nation's critical national infrastructure, the testbed needs to be able to report information, such as uncovered vulnerabilities, to the relevant authorities. This means that a testbed needs to have a connection in order to report information to the defence sector, government and organisations that maintain the CNI.

Specification 11: A test facility needs to have contacts with relevant authorities in order to guide the testing performed in terms of the national interest.

Specification 12: A test facility needs to be able to hold classified information and have the ability to report information such as critical vulnerabilities to the relevant authorities.

4.9 Support System-of-Systems Testing

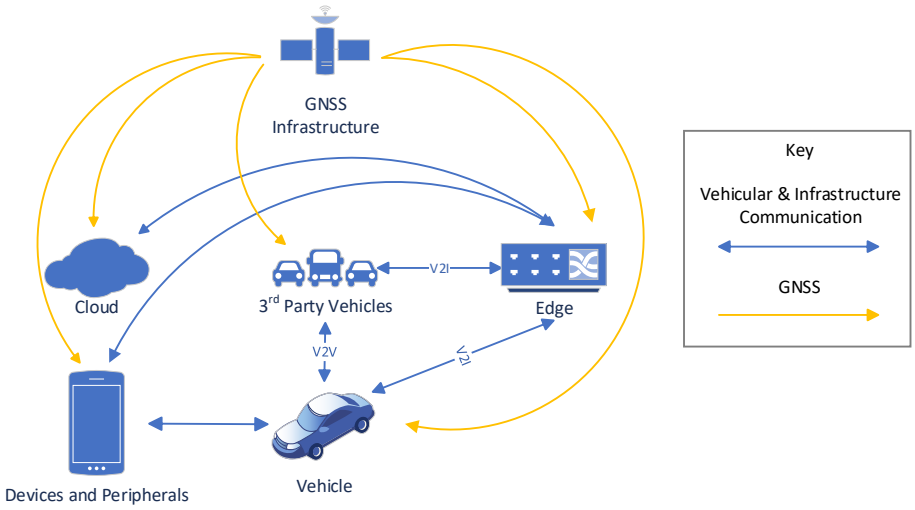


Figure 4.4: Reference Architecture showing vehicular system-of-systems [4]

> There seems to be a gap in UK capability in testing PNT at the system-of-systems level. For example, how can we fully test a system where inputs from multiple sensors, GNSS, Wi-Fi, Bluetooth, accelerometers and gyros are all blended together? Or how all the components of a car, fire engine or aircraft work together in all conditions and locations? On a sunny day in Oxfordshire, how do you conduct worst-case testing of the navigation and communications systems used by emergency services?
>
> *Government Office for Science, 2018 [6, p. 82]*

CAM systems are themselves a system-of-systems, as they contain many different interacting components. It is important to be able to test these systems considering the impact of other aspects of the system-of-systems, for example, how are other sensor inputs manipulated to reflect a GNSS attack that is being simulated? CAM systems also form a system-of-systems with the infrastructure they interact with, this includes the roadside infrastructure (such as traffic lights and communication devices), other CAM systems, and other services that are accessed via the internet. The relations and interactions between this system-of-systems are complex and need to be able to be tested under attack. For example, what impact will a stationary attacker have, which is spoofing GNSS for roadside units, on vehicles quickly moving through the region being spoofed? Testbeds need to support the testing of such complex scenarios.

Specification 13: A testbed should provide facilities that support testing of the PNT attack resilience of individual components and multiple interacting systems.

4.10 Test Facility Employees

As well as the technical specifications of a GNSS cyber-security testbed, it is also important to consider the requirements of the employed staff at testbeds. Employees at a testbed will need

broad skills in three key domains of radio frequency, automotive, and cyber-security. It was raised during our interviews that having employees with the right training is crucial.

Radio frequency skills are required in order to understand the physical layer and related technical details of a GNSS signal attack, including the test and measurement methods that will be used and how the attacks can be legally emulated.

Automotive skills are important in order to apply the use of GNSS-provided PNT to relevant automotive systems. More specifically, knowledge is required about how CAM systems use PNT and what expected fallbacks are if information is unavailable or incorrect.

Cyber-security skills are required in order to identify which threats are high priority to focus. This means identifying adversaries and their motivations, goals, capabilities and other aspects. These skills will also ensure correct disclosure procedures are followed if critical vulnerabilities are discovered.

Specification 14: Employees at test facilities need to have skills in RF, cyber-security and automotive.

When running a cyber-security testbed it is important to perform vetting of employees to mitigate potential risks. This also includes managing risks posed by contractors and support staff, such as being exposed to sensitive information and insider threats.

Specification 15: Employees at test facilities need to be suitably vetted, and risks posed by employees and contractors (i.e. insider threat) need to be appropriately managed.

4.11 Standards for GNSS Testing

> “The main problem in this area is that there are no published performance standards that could be used directly to compare the resilience and robustness of one GNSS receiver or system against another. Instead, purchasers must rely on manufacturer specifications, or conduct their own comparative evaluation testing.”
>
> *Government Office for Science, 2018 [6, p. 78]*

It is important to consider both attacks which threat actors are capable of performing now, as well as attacks that adversaries are not yet capable of, but may become capable of in the near future. Identifying the changes that will lead to novel attacks in the future is challenging, so it is important to monitor the evolving threat landscape. An impact analysis of these threats will need to be performed in order to prioritise those with greatest effects on CAM systems.

Recommendation 2: A set of standards needs to be created to measure the resilience of PNT attacks against CAM systems.

The European Committee for Standardization (ECS) is currently developing EN 16803-3 [31] which is a draft standard for assessing the security of GNSS receivers. The British Standards Institution (BSI) makes this draft standard available for UK stakeholders to engage with providing comments to the ECS. While this document provides useful guidelines on jamming and spoofing attacks, there is no consideration of software attacks. However, the draft standard does include a focus on testing vehicles equipped with GNSS receivers. Zenzic, Spirent and WMG should consider using lessons learnt in this project to feed into this standard.

4.12 Subscribe to GNSS Threat Monitoring and Reporting

There are a number of bodies that report on detected GNSS threats such as the US Coast Guard and the ITU [21]. Information from these bodies should be subscribed to so that GNSS testing for CAVs is up-to-date with current state-of-the-art attacks being used in the wild. GNSS cyber-security testing standards should be periodically revised to take into account changes in the detected attacks currently being performed. Recommendations from the STRIKE3 project on threat reporting [12] could be used as a basis for this system. This recommendation relates to TD09 in the Zenzic Roadmap [26, p. 97], as this information should be used to update the national threat database that TD09 proposes developing.

Recommendation 3: A test facility should subscribe to GNSS threat monitoring and reporting services and use the provided information to revise standards and testing strategies based on real-world incidents.

4.13 Facility Directory

> “However, there is no central register or database of UK facilities for PNT testing, making it difficult for an organisation to obtain information on where it can carry out work or whether testing is possible. Creating such a database will greatly improve awareness for all organisations, and lower the barriers to access for small to medium sized businesses.”
>
> *Government Office for Science, 2018 [6, p. 83]*

Following on from an issue highlighted in [6, p. 83], there is a lack of a suitable database of existing facilities to perform PNT-related testing. There are two issues here, the first is that additional information needs to be provided by other existing testbeds on their GNSS test supporting capabilities. It would be preferable for Zenzic to maintain a central database on these capabilities to simplify the process for interested parties to find appropriate test sites. The second issue is that non-automotive GNSS testing facilities may benefit from the sources available in automotive-focused testbeds and vice-versa. Efforts should be made to reach out to these facilities, for example, the MIMO chamber of the Satellite Applications Catapult in

Harwell, and the SMART chamber of the National Physical Laboratory in Teddington, in order to better integrate GNSS attack testing between automotive and non-automotive facilities.

Recommendation 4: Zenzic should maintain a directory of existing facilities and of their supported aspects of cyber-security testing.

4.14 Non-Automotive Testing

Multiple other domains exist which would benefit from the systematic organisation of GNSS testing facilities. The provision of an automotive GNSS PNTAE could potentially be expanded in order to facilitate the testing of related applications and equipment. This may include non-transport domains such as financial services, energy, communications, agriculture, infrastructure monitoring [6], or non-automotive transport areas such as aviation [6] and maritime [33].

Recommendation 5: A test facility should consider to facilitate testing classes of CAM beyond automobiles, such as UAVs, USVs and UUVs.

4.15 Conclusion

These specifications and recommendations have been made such that:

- There is a clear approach to performing testing (Specifications 1, 2, 8, 9 and 10 plus Recommendation 1),
- There is a method to evaluate the results (Specification 6 plus Recommendation 2),
- The equipment and environment needed to perform this testing is known (Specifications 3, 4 and 5) and well documented (Recommendation 4),
- Testing is relevant (Specifications 11 and 13 plus Recommendation 3),
- Detected issues can be reported (Specification 12),
- Testbed employees have relevant skills (Specification 14) and are sufficiently vetted (Specification 15),
- Testbeds should consider facilitating non-automotive testing (Recommendation 5).

These specifications and recommendations provide a path to facilitating more comprehensive and systematic testing of GNSS cyber-security for CAVs. Implementing these needs to be performed in collaboration with national and international bodies monitoring GNSS attacks (such as STRIKE3) and creating standards to measure resilience against attacks (such as ECS and BSI). There needs to be collaboration between automotive and non-automotive testing of GNSS cyber-security to reduce duplication of effort and to transfer knowledge between the different domains.

5 Conclusions

In this report we have presented specifications and recommendations for a GNSS cyber-security testbed for CAVs. These specifications and recommendations have been derived from:

1. Existing work which has made recommendations for testing,
2. A survey of academic literature on types of attacks and the techniques to detect and mitigate these attacks,
3. Interviews with experts in automotive, GNSS and cyber-security domains,
4. Our own experiences from performing testing in laboratory and real-world settings.

5.1 Findings

In recent years there has been an increased interest in improving the resilience of GNSS receivers against attacks such as spoofing and jamming. This has been demonstrated in projects such as STRIKE3, where practical evidence of GNSS jamming attacks were used to motivate standards for reporting of such events. The UK Government Office for Science also produced a Blackett review on satellite-derived time and position, focusing on the impact of GNSS attacks on aspects of the UK's CNI. As part of this report recommendations were made to improve the CNI's resilience to GNSS attacks.

In order to focus on CAV-specific threats and testing we interviewed experts in the automotive, GNSS and cyber-security community and performed our own testing on devices in both a laboratory and real-world setting.

Our interviews highlighted that attacks against GNSS are feasible for adversaries to perform and that there are incidences of them occurring in practise. It was also highlighted that there is no finalised standard available to measure resilience following a standard testing methodology (although this is being addressed by the ECS and BSI in [31]). The third key point raised was that to improve resiliency GNSS-provided PNT needs to be fused with other sensors on a vehicle and this can be expected to also be required on aspects of the infrastructure that forms part of ITS.

The results from the lab-based and real-world, live-sky work provided different, but complementary results. A plethora of ways to execute PNT attack scenarios exists, hence both lab-based and live testing require labour-intense work before all interesting parameters are investigated, and a complete and reliable conclusion on a system's PNT-attack resilience can be provided. In order to carry out the full range of Lab2Live tests, a PNT attack emulator, as used in this presented feasibility study, is an ideal component of a robust research methodology.

From this experience we developed a set of specifications and recommendations for a GNSS cyber-security testbed for CAVs and made the following three key findings:

1. Spoofing and jamming attacks on GNSS signals are capable of leading to severe loss of functionality and safety in CAVs by denying them access to or providing them with incorrect positioning, navigation, and timing information.
2. PNT testing facilities are urgently needed across a wide spectrum of capabilities, from simulation in artificial environments to over-the-air testing in labs and real-world environments. Procedures to legally perform real-world testing via OTA broadcasts need to be developed.

3. There is existing work on the standardisation of GNSS attack detection and GNSS resiliency assessment. Zenzic, UK CAV testbeds, the University of Warwick and Spirent should work with these bodies to guide the development of standards, and to further develop both attack event detection and responsible disclosure of information on threat actors and attack events.

5.2 Specifications and Recommendations

Throughout this report, specifications and recommendations have been made to inform CAV testbeds of what functionalities they need to provide as part of a GNSS cyber-security test facility. The specifications and recommendations that were made, fall into the following categories:

- There is a clear approach to performing testing,
- There is a clear method to evaluate the results,
- The equipment and environment needed for this testing is known and well-documented,
- Testbed employees have relevant skills and are sufficiently vetted.
- Detected issues can be reported,
- Potential future capabilities could allow testbeds to consider facilitating non-automotive GNSS cyber-security testing.

From the lessons learnt and findings of this project, and the derived specifications and recommendations for a GNSS cyber-security test facility for CAVs, it can be seen that threat actors, attack vectors, and required countermeasures will evolve. As a result, government and all associated stakeholders need to continue to work together to foster collaborative research and development that is capable of testing and certifying PNT for CAVs and CAM in the UK. The specifications for GNSS cyber-security test facilities made in this document will enable further testing of a critical aspect of CAVs, CAM and ITSs.

Bibliography

[1] M. Bradbury, E. Adegoke, E. Kampert, M. Higgins, T. Watson, P. Jennings, C. Ford, G. Buesnel, and S. Hickling. PNT Cyber Resilience: a Lab2Live Observer Based Approach, Report 2: Specifications for Cyber Testing Facilities. Technical Report 2, University of Warwick, Coventry, UK, April 2020. Version 1.2.

[2] E. Adegoke, M. Bradbury, E. Kampert, M. Higgins, T. Watson, P. Jennings, C. Ford, G. Buesnel, and S. Hickling. PNT Cyber Resilience: a Lab2Live Observer Based Approach, Report 1: GNSS Resilience and Identified Vulnerabilities. Technical Report 1, University of Warwick, Coventry, UK, April 2020. Version 1.0.

[3] E. Adegoke, J. Zidan, E. Kampert, C. R. Ford, S. A. Birrell, and M. D. Higgins. Infrastructure Wi-Fi for connected autonomous vehicle positioning: A review of the state-of-the-art. *Vehicular Communications*, 20: 100185, December 2019. ISSN 2214-2096. doi:10.1016/j.vehcom.2019.100185.

[4] C. Maple, M. Bradbury, A. T. Le, and K. Ghirardello. A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis. *Applied Sciences*, 9(23):5101, November 2019. ISSN 2076-3417. doi:10.3390/app9235101.

[5] J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, C. R. Ford, and M. D. Higgins. GNSS Vulnerabilities and Existing Solutions: A Review of the Literature. *IEEE Access*, pages 1–1, 2020. ISSN 2169-3536. doi:10.1109/ACCESS.2020.2973759.

[6] C. Whitty and M. Walport. *Satellite-derived Time and Position: A Study of Critical Dependencies*. London, UK, 30th January 2018. URL `https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/676675/satellite-derived-time-and-position-blackett-review.pdf`.

[7] M. Pattinson, S. Lee, Z. Bhuiyan, S. Thombre, V. Manikundalam, and S. Hill. Draft Standards for Receiver Testing Against Threats. Technical Report D4.2, STRIKE3, November 2017. URL `http://www.aic-aachen.org/strike3/downloads/STRIKE3_D42_Test_Standards_v2.0.pdf`. Issue 2.0.

[8] V. Murray. Legal GNSS Spoofing and its Effects on Autonomous Vehicles. In *Black Hat USA*, Las Vegas, NV, USA, 7th August 2019. Black Hat.

[9] F. Dimc, M. Bažec, D. Borio, C. Gioia, G. Baldini, and M. Basso. An Experimental Evaluation of Low-Cost GNSS Jamming Sensors. *Navigation*, 64(1):93–109, 2017. doi:10.1002/navi.184.

[10] P. J. G. Teunissen and O. Montenbruck, editors. *Springer Handbook of Global Navigation Satellite Systems*. Springer International Publishing, Gewerbestrasse 11, 6330 Cham, Switzerland, first edition, 2017. ISBN 978-3-319-42926-7. doi:10.1007/978-3-319-42928-1.

[11] R. Mitch, R. Dougherty, M. Psiaki, S. Powell, B. O'Hanlon, J. Bhatti, and T. Humphreys. Signal characteristics of civil GPS jammers. In *24th International Technical Meeting of the Satellite Division of the Institute of Navigation 2011, ION GNSS 2011*, 24th International Technical Meeting of the Satellite Division of the Institute of Navigation 2011, ION GNSS 2011, pages 1907–1919, 12 2011. ISBN 9781618394750.

[12] M. Pattinson, D. Fryganiotis, and P. Eliardsson. Draft Standards for Threat Monitoring and Reporting. Technical Report D4.1, STRIKE3, November 2017. URL `http://www.aic-aachen.org/strike3/downloads/STRIKE3_D41_Reporting_Standards_v2.1.pdf`. Issue 2.1.

[13] D. Borio, F. Dovis, H. Kuusniemi, and L. Lo Presti. Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers. *Proceedings of the IEEE*, 104(6):1233–1245, June 2016. ISSN 1558-2256. doi:10.1109/JPROC.2016.2543266.

[14] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang. All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 1527–1544, Baltimore, MD, August 2018. USENIX Association. ISBN 978-1-939133-04-5. URL `https://www.usenix.org/conference/usenixsecurity18/presentation/zeng`.

[15] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley. GPS Software Attacks. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 450–461, New York, NY, USA, 2012. Association for Computing Machinery. ISBN 9781450316514. doi:10.1145/2382196.2382245.

[16] A. Broumandan, R. Siddakatte, and G. Lachapelle. An approach to detect GNSS spoofing. *IEEE Aerospace and Electronic Systems Magazine*, 32(8):64–75, Aug 2017. ISSN 1557-959X. doi:10.1109/MAES.2017.160190.

[17] M. Z. H. Bhuiyan, N. G. Ferrara, A. Hashemi, S. Thombre, M. Pattinson, and M. Dumville. Impact Analysis of Standardized GNSS Receiver Testing against Real-World Interferences Detected at Live Monitoring Sites. *Sensors*, 19(6), 2019. ISSN 1424-8220. doi:10.3390/s19061276.

[18] M. Harris. Ghost ships, crop circles, and soft gold: A GPS mystery in Shanghai. *MIT Technology Review*, 15th November 2019. URL `https://www.technologyreview.com/s/614689/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/`. Accessed: 2020-01-15.

[19] E. Steindl, W. Dunkel, A. Hornbostel, C. Hättich, and P. Remi. The impact of interference caused by GPS Repeaters on GNSS receivers and services. In *European Navigation Conference*, ENC GNSS, Wien, Österreich, 22–25 April 2013. ISBN 978-3-200-03154-8.

[20] O. Towlson, D. Payne, P. Eliardsson, and V. Manikundalam. Threat Database Analysis Report. Technical Report D6.2, STRIKE3, January 2019. URL `http://www.aic-aachen.org/strike3/downloads/STRIKE3_D6.2_Threat_database_Analysis_Report_public_v1.0.pdf`. Issue 1.0.

[21] S. Thombre, M. Z. H. Bhuiyan, P. Eliardsson, B. Gabrielsson, M. Pattinson, M. Dumville, D. Fryganiotis, S. Hill, V. Manikundalam, M. Pölöskey, S. Lee, L. Ruotsalainen, S. Söderholm, and H. Kuusniemi. GNSS Threat Monitoring and Reporting: Past, Present, and a Proposed Future. *Journal of Navigation*, 71(3): 513–529, 2018. doi:10.1017/S0373463317000911.

[22] Resilient Navigation and Timing Foundation. Policy Recommendations for GPS/GNSS. URL `https://rntfnd.org/what-we-do/our-recommendations-gps-gnss/`. Accessed: 2020-02-25.

[23] Department for Business, Energy & Industrial Strategy, UK Research and Innovation, and Amanda Solloway MP. World's first timing centre to protect UK from risk of satellite failure , 19th February 2020. URL `https://www.gov.uk/government/news/worlds-first-timing-centre-to-protect-uk-from-risk-of-satellite-failure`. Accessed: 2020-02-26.

[24] Wireless Telegraphy Act 2006, 8th November 2006. URL `www.legislation.gov.uk/ukpga/2006/36`. Accessed: 2020-02-30.

[25] The Electromagnetic Compatibility Regulations 2016, 15th November 2016. URL `http://www.legislation.gov.uk/uksi/2016/1091`. Accessed: 2020-02-24.

[26] *UK Connected and Automated Mobility Roadmap to 2030*. Zenzic-UK Ltd., London, UK, 2019. URL `https://zenzic.io/content/uploads/2019/09/Zenzic_Roadmap_Report_2019.pdf`.

[27] Resilient Navigation and Timing Foundation. *Prioritizing Dangers to the United States from Threats to GPS: Ranking Risks and Proposed Mitigations*. Alexandria, VA, USA, 30th November 2016. URL `https://rntfnd.org/wp-content/uploads/12-7-Prioritizing-Dangers-to-US-fm-Threats-to-GPS-RNTFoundation.pdf`.

[28] Centre for Connected and Autonomous Vehicles. *Code of Practice: Automated vehicle trialling*. London, UK, February 2019. URL `https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/776511/code-of-practice-automated-vehicle-trialling.pdf`.

[29] N. Zhu, J. Marais, D. Betaille, and M. Berbineau. GNSS Position Integrity in Urban Environments: A Review of Literature. *IEEE Transactions on Intelligent Transportation Systems*, pages 1–17, 2018. ISSN 1524-9050. doi:10.1109/TITS.2017.2766768.

[30] D. Margaria, E. Falletti, and T. Acarman. The need for GNSS position integrity and authentication in ITS: Conceptual and practical limitations in urban contexts. *IEEE Intelligent Vehicles Symposium, Proceedings*, pages 1384–1389, 2014. doi:10.1109/IVS.2014.6856485.

[31] European Committee for Standardization. Draft BS EN 16803-3. Space. Use of GNSS-based positioning for road Intelligent Transport Systems (ITS). Part 3. Assessment of security performances of GNSS-based positioning terminals. Standard, Brussels, Belgium, 19 February 2019. Draft for public comment, Current.

[32] G. Mori Gonzalez, I. Petrunin, R. Zbikowski, K. Voutsis, and R. Verdeguer Moreno. Vulnerability Analysis of GPS Receiver Software. In *2019 International Conference on Localization and GNSS (ICL-GNSS)*, pages 1–6, June 2019. doi:10.1109/ICL-GNSS.2019.8752862.

[33] S. A. Shaikh. Future of the Sea: Cyber Security. Technical report, Government Office for Science, London, UK, August 2017. URL `https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/671824/Future_of_the_Sea_-_Cyber_Security_Final.pdf`.