

AUSTROADS TECHNICAL REPORT

Performance-based Specification for Electronic Work Diary and Heavy Vehicle Speed Monitoring (DRAFT FOR PUBLIC COMMENT)



**Performance-based Specification for Electronic Work
Diary and Heavy Vehicle Speed Monitoring
(DRAFT FOR PUBLIC COMMENT)**

Performance-based Specification for Electronic Work Diary and Heavy Vehicle Speed Monitoring (Draft for Public Comment)

Published October 2010

© Austroads Ltd. 2010

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without the prior written permission of Austroads.

Austroads Project No. FS1412

Performance-based Specification for Electronic Work Diary and Heavy Vehicle Speed Monitoring *(Draft for Public Comment)*

Program Manager

Philip Halton, Roads & Traffic Authority, New South Wales
(July 2007 – July 2009)
David Shelton, VicRoads, Victoria
(July 2009 – July 2010)
Nial Finegan, VicRoads, Victoria
(July 2010 onwards)

Project Manager

Philip Halton, Roads & Traffic Authority, New South Wales
(July 2007 – January 2010)
Daniel Kicuroski, Roads & Traffic Authority, New South Wales
(January 2010 onwards)

Prepared by

Chris Koniditsiotis, Charles Karl, Shaun Talko, Will Warner, David Cai and Jose Dang
Transport Certification Australia Ltd

Austroads Steering Group

Angus Draheim, QTMR
David Shelton, VicRoads
Don Hogben, VicRoads
Don Leone, VicRoads
Geoffery McMillan, QTMR
Greg George, Commonwealth DIT
Henry Schleimer, QTMR
John Jarrad, DTEI SA
Julie Cooper, VicRoads
Lindsay Oxlad, DTEI SA
Neil Wong, NTC
Robert de Maid, NTC
Stewart Jones, Commonwealth DIT
Tim Eaton, NTC
Chris Koniditsiotis, TCA

Consultants

Barry Moore
BeneflITS consulting
Damien Hill
Rapp Trans AG

Direct consultation participants

Austroads extends particular acknowledgement to the following:

LinFox Group Pty. Ltd., Toll Linehaul, Simon National Carriers, Victorian Transport Association, Woolworths, BlueScope Steel, Blackbox Control Pty. Ltd., Continental Pty. Ltd. (VDO), Fleet Effect Pty. Ltd., GPS Online Solutions Pty. Ltd., Minorplanet Asia Pacific Pty. Ltd., OmniSTAR Pty. Ltd., Optalert Pty. Ltd., Pinpoint Communications Pty. Ltd., Smart Car Technologies Pty. Ltd., Transtech Driven Pty. Ltd. and Transport Compliance Services Pty. Ltd.

Published by Austroads Ltd.
Level 9, Robell House
287 Elizabeth Street
Sydney NSW 2000 Australia
Phone: +61 2 9264 7088
Fax: +61 2 9264 1657
Email: austroads@austroads.com.au
www.austroads.com.au

Austroads believes this publication to be correct at the time of printing and does not accept responsibility for any consequences arising from the use of information herein. Readers should rely on their own skill and judgement to apply information to particular issues.

Performance-based Specification for Electronic Work Diary and Heavy Vehicle Speed Monitoring (DRAFT FOR PUBLIC COMMENT)



Austroads

Sydney 2010

Austroads profile

Austroads' purpose is to contribute to improved Australian and New Zealand transport outcomes by:

- providing expert advice to SCOT and ATC on road and road transport issues
- facilitating collaboration between road agencies
- promoting harmonisation, consistency and uniformity in road and related operations
- undertaking strategic research on behalf of road agencies and communicating outcomes
- promoting improved and consistent practice by road agencies.

Austroads membership

Austroads membership comprises the six state and two territory road transport and traffic authorities, the Commonwealth Department of Infrastructure and Transport, the Australian Local Government Association, and NZ Transport Agency. Austroads is governed by a Board consisting of the chief executive officer (or an alternative senior executive officer) of each of its eleven member organisations:

- Roads and Traffic Authority New South Wales
- Roads Corporation Victoria
- Department of Transport and Main Roads Queensland
- Main Roads Western Australia
- Department for Transport, Energy and Infrastructure South Australia
- Department of Infrastructure, Energy and Resources Tasmania
- Department of Lands and Planning Northern Territory
- Department of Territory and Municipal Services Australian Capital Territory
- Commonwealth Department of Infrastructure and Transport
- Australian Local Government Association
- New Zealand Transport Agency.

The success of Austroads is derived from the collaboration of member organisations and others in the road industry. It aims to be the Australasian leader in providing high quality information, advice and fostering research in the road sector.

CONTENTS

EXECUTIVE SUMMARY	IV
1 INTRODUCTION	1
1.1 Background.....	1
1.1.1 Regulatory context.....	1
1.1.2 Transport and telematics industry context	2
1.2 Scope of specification	2
1.3 Approach	3
1.4 The specification.....	4
1.5 Layout of report.....	5
2 CURRENT UTILISATION OF ELECTRONIC SYSTEMS	6
2.1 Transport industry use of electronic systems	6
2.2 Telematics industry provision of electronic systems.....	6
3 PHILOSOPHY OF THE SPECIFICATION	7
4 SPECIFICATION FOR THE ELECTRONIC WORK DIARY	11
4.1 EWD architecture and stakeholders	11
4.1.1 Driver Recording Device (DRD).....	12
4.1.2 In-Vehicle Unit (IVU)	12
4.1.3 Printer	13
4.1.4 Driver	13
4.1.5 Operator.....	13
4.1.6 Authority.....	13
4.1.7 Enforcement officer.....	13
4.1.8 Driver Recording Device (DRD) issuer	14
4.1.9 Record keeper	14
4.1.10 EWD Provider.....	16
4.1.11 System Manager.....	16
4.2 EWD operation	17
4.2.1 An EWD is approved, it incorporates an IVU and the ability to insert a DRD	17
4.2.2 An IVU is installed in the heavy vehicle	17
4.2.3 The driver identification and authentication method for the IVU	18
4.2.4 The driver applies for and is issued with a Driver Recording Device (DRD).....	18
4.2.5 The driver keeps the DRD	18
4.2.6 EWD records	18
4.2.7 The driver is aided by the EWD which creates electronic records of work and rest (declared by driver).....	19
4.2.8 Two-up driver situation (corroboration declared by second driver).....	19
4.2.9 Monitoring of IVU	20
4.2.10 The driver's records are available to the Authority and enforcement officer.....	20
4.2.11 The records are available to the driver and the record keeper	20
4.3 EWD information recorded	21
5 EQUIVALENCE BETWEEN WWD AND EWD	23
5.1 Technical equivalence	23
5.2 Operational equivalence	23

5.2.1	General.....	23
5.2.2	Business process.....	23
5.2.3	Features.....	25
5.3	Stakeholder equivalence	28
5.3.1	WWD environment.....	28
5.3.2	Specified EWD environment.....	29
5.4	Overall equivalence	31
6	SPECIFICATION FOR HEAVY VEHICLE SPEED MONITORING	33
6.1	Speed monitoring architecture and stakeholders	33
6.2	Speed monitoring operation.....	33
6.2.1	Speed monitoring system is approved.....	33
6.2.2	Speed monitoring system is installed in the heavy vehicle.....	34
6.3	Driver identification and authentication.....	34
6.3.1	Speed monitoring system electronic records.....	34
6.3.2	Speed monitoring system automatically generates Speed records.....	34
6.3.3	The electronic records are available to the operator	34
6.3.4	Monitoring of IVU	35
6.4	Speed monitoring information recorded.....	35
7	UNRESOLVED ISSUES.....	36
7.1	Stakeholder issues	36
7.2	Technical issues	37
7.2.1	Interoperability	37
7.2.2	Multiple application environment	38
7.2.3	Printer	39
7.2.4	Accurate and reliable recording of location and date/time	40
7.2.5	Automatic capture and populate records.....	40
7.2.6	Location records	41
7.2.7	IVU is tethered to vehicle.....	41
7.2.8	Tamper monitoring.....	42
7.2.9	Time recording resolution	42
7.3	Possible future extended regulatory uses.....	42
8	WHAT NEEDS TO HAPPEN NEXT?	44
8.1	Consultation.....	44
8.2	Operational pilot.....	44
8.3	Dealing with operator legacy electronic systems.....	45
	REFERENCES	47
	SPECIFICATION DOCUMENT	A - I
	APPENDIX A – SPECIFIED EWD	A - 1
	APPENDIX B – NTC POSITION ON THE EWD	A - 32
	APPENDIX C – NTC POSITION ON HEAVY VEHICLE SPEED MONITORING	A - 43
	TERM & DEFINITIONS	A - 50

FIGURES

Figure 1: Structure of the report.....	5
Figure 2: Specified EWD system	12
Figure 3: Specified EWD system - employer as the record keeper	14
Figure 4: Specified EWD system – driver (self-employed) as record keeper.....	15
Figure 5: Specified EWD system – operator as the record keeper.....	16
Figure 6: WWD business process.....	24
Figure 7: Specified EWD business system	25
Figure 8: Key stakeholders in the WWD environment	29
Figure 9: Key stakeholders in the Specified EWD environment	30
Figure 10: Speed monitoring system	33
Figure 11: Various IVU configurations	39
Figure 12: Possible roadmap of the next steps.....	44
Figure 13: Approval process for transitional arrangement	47

TABLES

Table 1: Comparison of the system requirements	9
Table 2: EWD record - Detail record.....	21
Table 3: EWD electronic record - Work record	22
Table 4: WWD and the Specified EWD feature 'case' equivalencies	27
Table 5: Speed monitoring information	35
Table 6: Unresolved stakeholder issues	36
Table 7: Unresolved technical issues	37
Table 8: Contents of location record	41
Table 9: Possible future extended regulatory uses.....	42
Table 10: Key issues for transitional arrangements	46

EXECUTIVE SUMMARY

Introduction

Transport Certification Australia (TCA) is pleased to present this draft specification report for a regulatory fatigue and heavy vehicle speed monitoring application. These specifications are based on the Fatigue and Speed Management System Requirements, Heavy Vehicle Driver Fatigue Model Legislation (HVDF Legislation) and constructive discussions held with Jurisdictions, the transport industry and the telematics industry.

This report is the third key milestone and deliverable identified by Austroads for the fatigue and speed monitoring project. After a public consultation process and further refinement, this report will form the basis of the functional and technical specification for Electronic Work Diary (EWD) and Heavy Vehicle Speed Monitoring.

Background

The recording of fatigue information is currently undertaken through a written work diary (WWD). The HVDF Legislation allows for the use of electronic record keeping devices, also known as Electronic Work Diaries (EWD). An enabling specification is required for Authorities to be able to consider fatigue management delivered through electronic systems.

The Australian Transport Council (ATC) at its November 2008 meeting directed the immediate development of an Australian performance-based specification for electronic heavy vehicle speed and driver fatigue systems, enhancing the use of in-vehicle telematics and adding value to the Intelligent Access Program (IAP). Through the direction of the ATC, Austroads requested that Transport Certification Australia (TCA) undertake a study to develop a draft performance-based specification for the fatigue management (essentially the electronic work diary) and monitoring of heavy vehicle speed.

This report was originally delivered to Austroads in November 2009. It contains the full details of a device which meets the terms of the Austroads contract with TCA, and includes requirements for a sustainable telematics platform suitable for possible future extended regulatory use.

The specified EWD fulfils the requirement for an electronic work diary that has the equivalent security, integrity and accuracy requirements expected of a work diary as stated in the HVDF legislation and evidenced in the written work diary and all its processes. It can be found in Appendix A.

The NTC position was that particular records were to be kept, but the option of doing so could be with either a WWD or through electronic record-keeping. In other words, the NTC's position was that the EWD should be, at minimum, merely an electronic version of the WWD, without GPS, but with a printer, so written records could be produced at the roadside.

In order to resolve the differences in the NTC approach, NTC requested that TCA second their project manager to the NTC to provide assistance with determining the areas of difference and to align the work packages.

The Specified EWD was subsequently reviewed to correspond to the preferred policy position presented in the NTC's position paper. This has resulted in an EWD and a separate heavy vehicle speed monitoring device based on the NTC position and presented as Appendix B and Appendix C.

This report is divided into eight sections. Figure ES - 1 details the structure of this report together with the appendices which are in a separate document. This document presents the Specified EWD and a version of an EWD and separate speed monitoring device that corresponds to the preferred policy position presented in the NTC's position paper. The documents are:

1. Appendix A – Performance Based Specification for Electronic Work Diary and Heavy Vehicle Speed (TCA 2009b).
2. Appendix B – NTC position on the EWD.
3. Appendix C – NTC position on heavy vehicle speed monitoring device.

The NTC positions are sub-sets of the EWD specification. The differences between the NTC positions and the Specified EWD are discussed later, as unresolved issues for consultation.

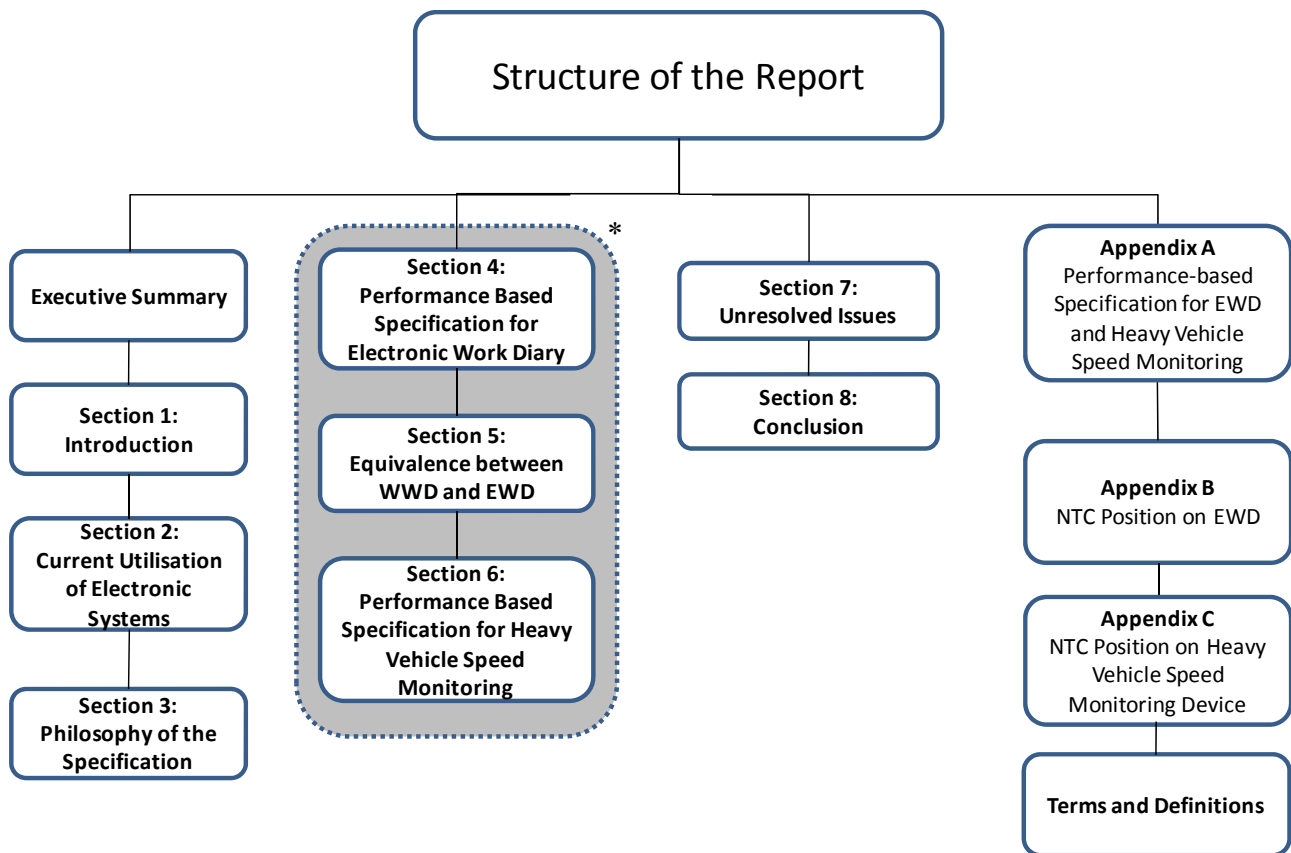


Figure ES - 1: Structure of the report

* The specifications outlined in Sections 4, 5 and 6 of this report have been restructured to provide the policy position of the NTC.

Methodology

TCA commenced this study by firstly seeking to fully identify all of the requirements of the electronic work diary from the HVDF Legislation as well as through developing an understanding of how the current written work diary operates.

TCA's initial approach was firstly, to clearly establish the requirements of an electronic version of the work diary. In July 2009, a Requirements Report was presented to the Austroads Steering Group (Steering Group) for confirmation, and in cases where the requirements remained unresolved, for guidance and direction.

The Austroads Steering Group was able to provide clarity on a number of these choices, but were unable to answer some of the more technical issues. Two Steering Group meetings were held in July and August to address the outstanding unresolved issues.

A further approach taken by TCA was to determine what an overall EWD system should incorporate in order for it to function as required. This approach enabled all of the tasks, functions, roles and entities to be recognised.

Additionally, as was directed by the ATC, where applicable a significant amount of experience and understanding developed with the Intelligent Access Program Functional and Technical Specification (IAP F&T Specification) was incorporated into the Performance Based Specification for Electronic Work Diary and Heavy Vehicle Speed Monitoring.

Current utilisation of electronic systems

The study found that some transport operators had acquired or developed electronic fatigue and heavy vehicle speed monitoring solutions. These relied on in-vehicle telematics and back office systems. These electronic systems ranged from out-sourced bureau to in-house solutions. Through consultation, the study determined a number of motivational factors for the transport industry adopting electronic approaches:

- The need to streamline and integrate driving, working (not driving) and rest monitoring as part of the entire 'track and trace' solution within fleet management. Driver working information is used for company operational purposes such as payroll and rostering.
- The use of electronic fatigue monitoring was considered better than paper with respect to integrity of the information collected. There was a general belief that the information in a written work diary was less accurate.
- The use of speed monitoring to ensure compliance of drivers to company operational policies.

The study found a number of providers of in-vehicle telematics claiming that their systems met the requirements of heavy vehicle driver fatigue regulations.

Overview of the Specified EWD

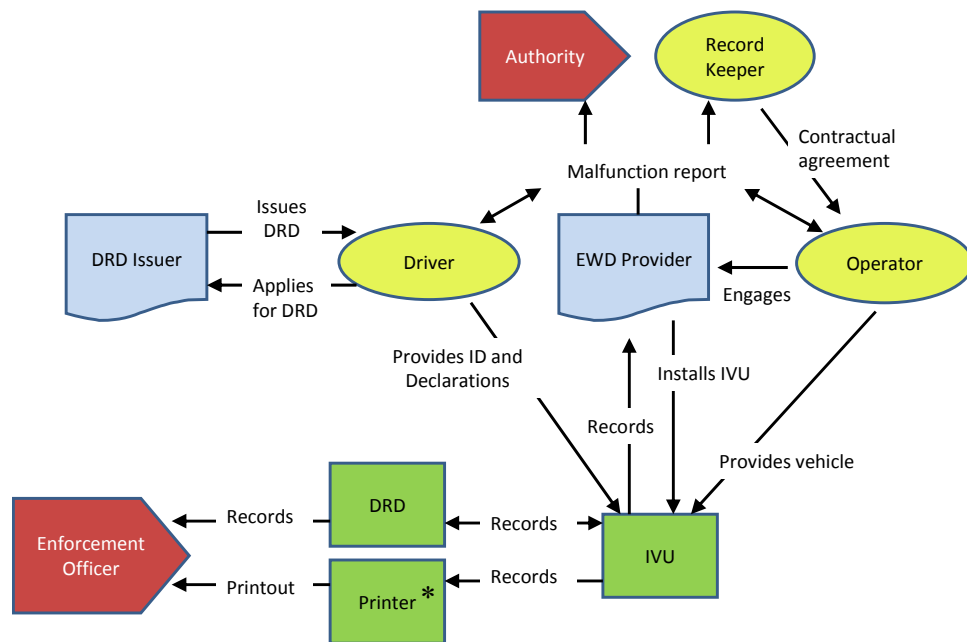
The Specified EWD with the roles, tasks and entities combined in one diagram, is shown in Figure ES - 2.

The **EWD Provider** collects records and provides services in reporting to potentially all approved entities in the chain of responsibility (Transport Operators, Authorities, drivers).

The EWD Provider is also responsible to report to the **System Manager** of the overall EWD system in the discharge of responsibilities related to certification and auditing.

The **in-vehicle unit** and the **driver recording device** are the technical components of the EWD system out in the field and used by drivers in compliance to the HVDF Legislation.

The driver recording device is interoperable across IVUs and as a result is able to be accessed by enforcement officers at the roadside.



* The printer is included in order to meet the policy position of the NTC.

The key features of the paper and electronic work diary as specified are detailed in Table ES – 1.

Table ES - 1: Features of the work diary in paper and electronic form

Feature	Written Work Diary	Specified Electronic Work Diary
1. Allocation (1 diary per driver)	- Diary only available from Authority - Diary number linked to driver	- IVU only available from EWD Provider - Driver Recording Device (DRD) only available from DRD Issuer - DRD identifier is linked to driver
2. Authentication	- Driver signature - Driver's licence number	Method is consistent with Australian Government Standard for identification and e-authentication
3. Records cannot be deleted	- Records are entered in ink - Each page is sequentially numbered	- Driver Recording Device: security prevents records being deleted - IVU: has seals and alarms
4. Records cannot be changed	- Tampering is visible - Pages can be forensically checked - Records are in triplicate	- Use of digital signatures to show author and evidence of change - There is a known set of approved digital signatures
5. Records are duplicated	Immediate duplication of pages	Records are saved onto DRD and copies transferred to EWD Provider.
6. System is functional	The diary is always functional	- Indicator on IVU shows system OK. - IVU creates alarms - System maintained by EWD Provider

Unresolved issues

The philosophy underpinning the HVDF Legislation was based on a paper environment. Obviously a paper and electronic environment do not exactly match one to one. As such, moving to an Electronic Work Diary environment has resulted in a number of functional and business process challenges.

The Specified EWD is a device which meets the terms of the Austroads contract with TCA, and includes requirements for a sustainable telematics platform suitable for possible future extended regulatory use. In doing so, some requirements that add greater integrity to the system extend beyond the policy position being recommended by the NTC which corresponds to the performance provided by a written work diary.

The key differences in the requirements of the HVDF Legislation, the NTC position, the Specified EWD and potential future regulatory uses are detailed in Table ES – 2. The comparison reveals that the key differences are in fact technical and related to the overall integrity of the electronic system. Such technical differences are expected to be addressed and resolved through the upcoming consultation process.

Significantly, both the Specified EWD and the NTC position are the same with regards to the roles required in an electronic environment. What needs to be resolved is who is going to perform these functions. It is expected that the entities that perform the agreed roles will most likely have their own views on how the technical differences should be resolved.

Finally Table ES - 2 also compares the potential uses of the electronic records. Records collected by the work diary can and are being used today by drivers, transport operators and the Authorities. How such records can be used in the electronic world, over and above the way they are now, e.g., transmitting records electronically to the Authority in case of breaches, are matters that are unresolved and go beyond this report.

Table ES - 2: Key differences

System aspect		HVDF Legislation	NTC position	Specified EWD	Possible future extended regulatory uses
Roles	EWD Provider	Not required	Required	Required	Required
	DRD Issuer	Not required	Required	Required	Required
	System Manager	Not required	Required	Required	Required
Technical	Interoperability	Not required	Required	Required	Required
	Multi-application environment	Not required	Required	Required	Required
	Paper at roadside	Required	Required	Not required	Not required
System integrity	GPS in in-vehicle unit (IVU)	Not required	Not required	Required	Required
	Automatic capture and populate records	Not required	Not required	Required	Required
	Continuously capture position records	Not required	Not required	Required	Required
	IVU is tethered to vehicle	Silent	Not required	Required	Required
	Tamper monitoring	Required*	Not required	Required	Required
	Time recording resolution	15 minutes	1 minute	1 second	Required
Use of records	Advise drivers how much time remains before a rest break is due, in order to manage compliance.	Not required	Not required	Recommended	Required
	Report breaches and impending breaches to operators, allowing intervention prior to an offence.	Not required	Not required	Not required	Required
	Report instances of gross non-compliance directly to the authority, allowing for intervention by enforcement officers.	Not required	Not required	Not required	Required

* The HVDF legislation requires that drivers comply with the instructions of the Authority. Instructions for using the WWD state that the driver must report all tampering to the Authority within 2 business days.

Next steps

The revised Austroads Specification will be progressed through the Austroads approval process, and the NTC document will be finalised and approved for joint release before the August SCOT meeting. A joint consultative process will then be undertaken. As a result of this consultation, a final position will be reached which can be recommended to Ministers at ATC. The proposed pilot of electronic work diaries (to be led by NSW) will be needed to resolve some key points – particularly relating to the need for a capacity for in-vehicle printing.

A series of steps are proposed as a setting for going forward. Figure ES – 3 provides a possible roadmap of the next steps depicting the phasing of the operational pilot, arrangements for legacy systems together with the consultation process as well as the process to resolve the unresolved issues.

The roadmap proposes three distinct phases leading to a fully tested Specified EWD and heavy vehicle speed monitoring system becoming available to stakeholders based on an operational pilot (2010-2012) followed by period for the transition of legacy systems.

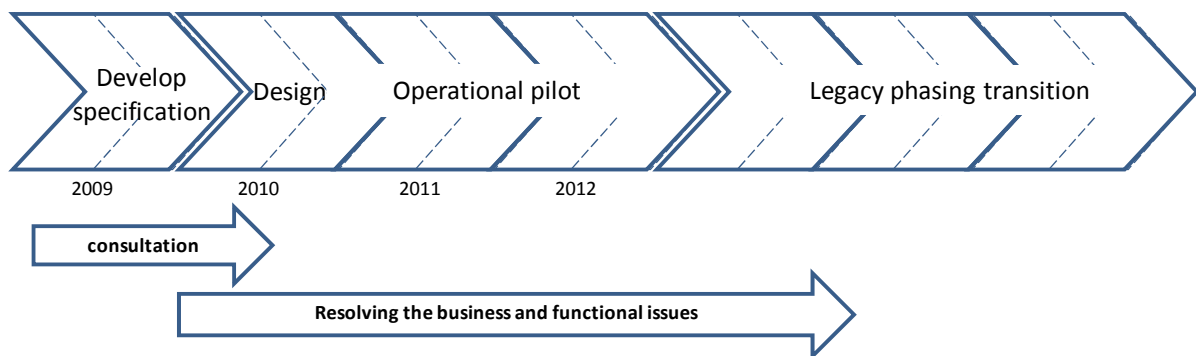


Figure ES - 3: Approval process for transitional arrangement

Consultation

Austroads seeks for stakeholders to consider the operation of the EWD as described within this document and the performance-based specification for the EWD and heavy vehicle speed monitoring system and provide input.

The consultation process will involve presentations and meetings with Authorities, presentations and meetings with transport industry groups (and associated Authority) and presentations and meetings with telematics industry and developers.

Throughout consultation with stakeholders, it was recognised that with the investment made by some operators to electronic systems, consideration should be given to permitting legacy phasing arrangements (i.e. transition), as part of achieving the Specified EWD and heavy vehicle speed monitoring systems.

Summary

In summary, prior to the implementation of the Specified EWD and heavy vehicle speed monitoring systems, the following steps should be considered:

Now

- Consultation with stakeholders on the draft performance-based specification and refinement of requirements.
- Undertaking of an operational pilot of no less than 18 months duration. The operational pilot should not be seen as testing the technology, but rather the business systems, human interaction and institutional processes in which the technology will exist.

Afterwards

- Arrangements dealing with operator legacy electronic systems that monitor fatigue and speed can be considered by Authorities.
- Agreement and allocation of entities to a number of roles necessary to operate an EWD and heavy vehicle speed monitoring system. In particular, the specification allocates functions under the roles of a EWD Provider, Driver Recording Device (DRD) issuer and System Manager. The specification makes no recommendation on actual entities to perform the identified roles, nor if some functions can be performed by the same entity.
- Consideration and possible amendment of the HVDF Legislation to explicitly permit the operational environment of the Specified EWD.

1 INTRODUCTION

The Australian Transport Council (ATC) at its November 2008 meeting directed the immediate development of an Australian performance-based specification for electronic heavy vehicle speed and driver fatigue systems, enhancing the use of in-vehicle telematics and adding value to the IAP. Austroads subsequently engaged Transport Certification Australia (TCA) to develop a draft performance-based specification for the fatigue management (commonly known as the electronic work diary) and the monitoring of heavy vehicle speed.

This report presents the Performance-based specification for Electronic Work Diary and heavy vehicle speed monitoring.

1.1 Background

1.1.1 Regulatory context

The Heavy Vehicle Driver Fatigue regulations took effect in Queensland, New South Wales, Victoria and South Australia in September 2008. They were based on the Heavy Vehicle Driver Fatigue National Model Legislation (HVDF Legislation) (NTC 2008).

These laws provide operators, employers and drivers with three options for fatigue management, as follows:

1. Standard Hours – which provides basic work and rest limits.
2. Basic Fatigue Management – which provides more flexible work and rest hours linked to operator accreditation and training of drivers.
3. Advanced Fatigue Management – which provides the ability to create one's own safety management system and work hours, within defined limits, linked to operator accreditation and training of drivers.

The recording of work and rest hours is currently undertaken through a written work diary (WWD). The HVDF Legislation allows for the use of electronic record keeping devices, also known as electronic work diaries (EWDs).

The HVDF Legislation imposes duties and accountabilities on all parties in the supply chain to manage the causes of heavy vehicle driver fatigue and to achieve compliance with applicable limits to hours of work and rest. These duties-based elements of the HVDF Legislation require off-road parties to take 'reasonable steps' not as a defence in the face of possible charges but as an obligation in and of itself.

More than any previous road transport law, the duties-based element of these fatigue laws creates an affirmative onus on the responsible parties to actively seek out information regarding levels of fatigue risk and compliance with work hours and to exercise control over these factors.

Complementing the HVDF Legislation, the ATC has recently approved new 'Chain of Responsibility' laws in connection with heavy vehicle speeding (NTC 2008d). These laws are similarly framed around affirmative duties.

To varying degrees, Authorities have had the ability to allow for electronic record keeping since 1999. However, Authorities have not had the capability to approve an electronic record keeping system. This is due to the HVDF Legislation not containing sufficient detail to fully consider the electronic environment. This is not unexpected, as the philosophy underpinning the HVDF Legislation assumes a paper based environment. For example, the HVDF Legislation is silent on:

- Who supplies the EWD and the responsibilities of the EWD supplier.
- How a driver should authenticate their declarations within the EWD environment.
- How drivers' records are transferred between vehicles and transport operators; and how drivers' records are presented to the enforcement officer.
- What the specification for the EWD is.

In the case of the written work diary, the answers to these questions are clearly given (prescribed) in the HVDF Legislation. Therefore for the electronic work diary, these are the unresolved issues. These issues are raised and discussed in this document. Going forward, these issues will need to be taken to consultation.

1.1.2 Transport and telematics industry context

A number of operators utilise commercial electronic record keeping systems that are not approved as electronic work diaries. These electronic systems provide information about the work and rest of the driver which can provide valuable information to assist operators in better managing their operations or could solely be used to assist in managing driver fatigue.

The use of electronic record keeping systems in addition to the WWD presents operators with two problems. In the first instance, the double handling of data is inefficient and the storage of paper records can be considered archaic in this day and age. In the second instance, the data recorded by one system may not necessarily be consistent with that of the other. It could be argued that this requires operators to have audit systems in place to consider instances where the two sets of data are not consistent.

The issue of the HVDF Legislation not providing sufficient detail to fully consider the electronic environment has also affected those in the telematics industry wishing to have their products approved as electronic work diaries. For the same reason that there is insufficient detail for Authorities to approve electronic work diaries, there is insufficient detail for the telematics industry to fully develop electronic work diaries. This highlights the problem for the operator wishing to invest in telematic equipment but not knowing if the system they are investing in will be able to be recognised as a replacement for the WWD.

1.2 Scope of specification

For Authorities, the transport industry and the telematics industry to be able to consider fatigue and speed management delivered through an electronic environment requires an enabling functional and technical specification. Such a specification would enable the provisions within HVDF Legislation and allow the telematics industry to develop and supply, Authorities to approve, and transport industry to utilise electronic work diaries with confidence.

The ATC at its November 2008 meeting requested:

'the immediate development of an Australian performance-based specification for electronic heavy vehicle speed and driver fatigue systems, enhancing the use of in-vehicle telematics and adding value to the Intelligent Access Program.'

The ATC's directive was in recognition of the increasing use of telematics by Authorities and the transport industry and the operational benefits that telematics use provides operators to comply with regulations, to complement accreditation systems, to increase compliance and reduce enforcement costs. Further, the use of electronic data presents an opportunity for Authorities and operators to review their approach to compliance. It brings the potential for real time alerting to drivers of impending breaches of fatigue regulations and provision of real time driver information to operators. For Authorities, it brings opportunities to reduce the frequency of, or time required to conduct compliance checks.

Responding to the ATC's directive, Austroads engaged the advisory, technical and operational expertise of TCA to develop a draft performance-based specification for the EWD and heavy vehicle speed monitoring systems.

The ATC has not mandated any regulated use of EWD or heavy vehicle speed monitoring. As such, the purpose of the specification was not to further develop nor modify fatigue or speed policy dimensions. The specification aimed to provide an electronic alternative to what is currently performed using a paper based approach.

1.3 Approach

In formulating the requirements for the Specified EWD, TCA was guided by an Austroads project Steering Group consisting of senior representatives from the Commonwealth and jurisdictions' road authorities to provide direction where operational or institutional issues arose. TCA also undertook other external consultation with industry and government. The Austroads contract further required TCA to use, as far as possible, existing elements of the Intelligent Access Program (for which TCA owns the intellectual property rights) as a basis for the specification.

In carrying out its role, the Austroads Steering Group necessarily provided direction which reflected particular policy positions. These have not in all instances been the same as those reached by the NTC. The parallel development and differences in guidance in formulating the work packages resulted in a divergence between the emerging preferred policy outcomes from the NTC process and the architectural requirements of the Specified EWD.

Prior to writing specifications, it was essential to determine what performance is required of the work diary under the HVDF Legislation. TCA commenced by identifying the requirements of the EWD from the HVDF Legislation as well as through understanding of how the WWD currently operates (TCA 2009a).

A further approach taken by TCA was to determine what an overall EWD and heavy vehicle speed monitoring system should incorporate in order for it to function as required. This approach enabled all of the tasks, functions, roles and entities to be recognised, regardless of whether or not they were present within the HVDF Legislation.

The HVDF Legislation allows for a work diary to be either paper based or electronic and provides a prescriptive description of the obligations for the driver of a heavy vehicle together with other entities within the chain of responsibility (CoR). The HVDF Legislation envisages an electronic form of the WWD, but remains silent on many of the operational processes that are present within the WWD which should obviously be replicated in some format for the EWD to perform in the same manner.

In July 2009, a Requirements Report was presented to the Austroads Steering Group (Steering Group) for confirmation, and in cases where the requirements remained unresolved, for guidance and direction (TCA 2009a). The Austroads Steering Group was able to provide clarity on a number of these choices, but was unable to answer some of the more technical in nature. Four full day Steering Group meetings were held in 2009 to address the outstanding unresolved issues.

One significant direction from the Austroads Steering Group was that the EWD system should maintain an equivalent evidentiary standard to the WWD. To achieve this directive, the HVDF Legislation was further examined to determine what evidence is required to support the offences described in the HVDF Legislation and then investigate how the WWD protects this evidence (BeneflITS 2009). A range of engineering controls to provide the most practicable electronic equivalent protection were recommended and developed within the specification.

The Draft Electronic Work Diary Specification was delivered to Austroads in November 2009 (TCA 2009b, c). It contained the full details of a device which meets the terms of the Austroads contract with TCA, and includes requirements for a sustainable telematics platform suitable for possible future extended regulatory use (Appendix A). In doing so, some requirements that add greater integrity to the system extend beyond the policy position being recommended by NTC.

Subsequent events in 2010

The NTC position was that particular records were to be kept, but the option of doing so could be with either a WWD or through electronic record-keeping. In other words, the NTC's position was that the EWD should be an electronic version based on the WWD, without GPS, but with a printer, so written records could be produced at the roadside.

In order to resolve the differences in the NTC approach, NTC requested that TCA second their project manager to the NTC to provide assistance with determining the areas of difference and to align the work packages.

The Specified EWD (TCA 2009b, attached as Appendix A) was subsequently reviewed to correspond to the preferred policy position presented in the NTC's position paper. This has resulted in two further documents; an EWD and a separate heavy vehicle speed monitoring device based on the NTC position (Appendix B, Appendix C).

1.4 The specification

This document presents the Specified EWD and a version of an EWD and separate speed monitoring device that corresponds to the preferred policy position presented in the NTC's position paper. These are presented as follows:

1. Appendix A – Specified EWD (TCA 2009b).
2. Appendix B – NTC position on the EWD.
3. Appendix C – NTC position on heavy vehicle speed monitoring device.

The NTC positions on EWD and heavy vehicle speed monitoring device are sub-sets of the Specified EWD.

The Specified EWD is outlined in Appendix A. The differences between the NTC positions and the Specified EWD are detailed in Section 7 as unresolved issues.

The reader is directed to begin by reading the Specification for Electronic Work Diary and Heavy Vehicle Speed Monitoring (Appendix A) as it is expected to best inform the reader about what is necessary for a fully-functional system. The NTC positions in Appendices B and C are best understood once the reader is aware of the specified all-encompassing solution.

1.5 Layout of report

Following this introductory section, this report contains:

- Section 2 - a précis of the current utilisation of electronic systems
- Section 3 - the philosophy of how the draft specification was developed
- Section 4 - a summary of the Specified EWD, highlighting the stakeholder – players, the mode of operation and information recorded within the system
- Section 5 - an assessment of the electronic equivalence to the WWD
- Section 6 - a summary of the heavy vehicle speed monitoring system, highlighting the stakeholder – players, its operation and information recorded
- Section 7 – unresolved issues
- Section 8 – conclusion and the next steps.

Figure 1 details the structure of this report.

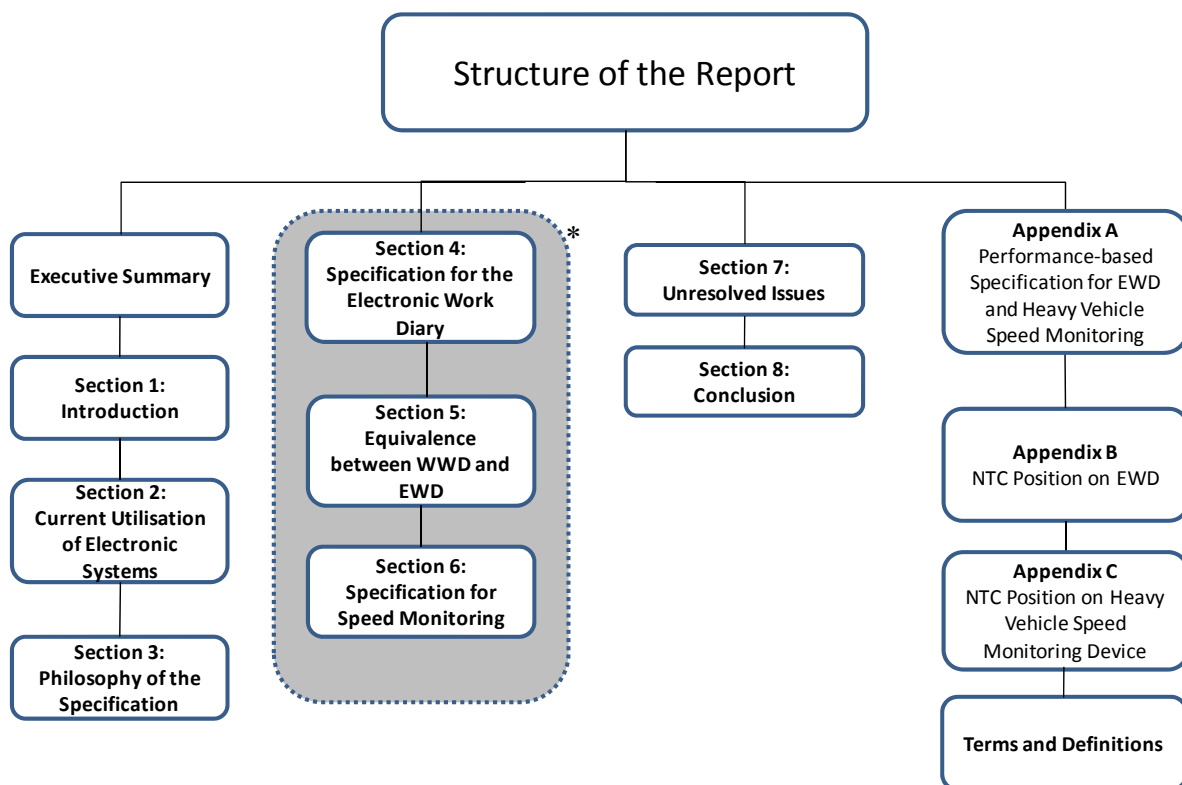


Figure 1: Structure of the report

* The specifications outlined in Sections 4, 5 and 6 of this report have been restructured to correspond with the policy position of the NTC.

2 CURRENT UTILISATION OF ELECTRONIC SYSTEMS

2.1 Transport industry use of electronic systems

In developing the specification, it was observed that some operators had acquired or developed commercial electronic record keeping systems. The majority of such systems relied on in-vehicle telematics approaches (i.e. an in-vehicle unit (IVU) and a back office system), and ranged from outsourced bureau services to in-house solutions. Through consultation, some of industry's motivations for adopting these systems were identified as follows:

- The need to streamline and integrate driving and non-driving work and rest monitoring as part of the entire in-vehicle telematics 'track and trace' solution. The transport industry uses the driver's information for company operational purposes such as scheduling trips, loading and unloading and general resource management.
- The use of in-vehicle telematics was considered to produce information of better integrity than paper. This information was also available in near real time rather than only at the end of the trip. There was a general belief that the WWD can be subject to error or deliberate false declarations making the information useless for business and operational decision needs.
- The use of speed monitoring to ensure compliance of the driver to company operational policies.

As mentioned above, most electronic monitoring solutions identified rely on in-vehicle telematics approaches, where date, time and location is independently determined, rather than being reliant on driver declaration.

It was also observed that some operators were scanning the pages of the written work diary into electronic format in order to further utilise the information contained in the WWD for a range of administrative, operational and record keeping requirements. In all cases, these operators then faced the challenge of reconciliation of information from the WWD and from their commercial record keeping and fleet management systems.

2.2 Telematics industry provision of electronic systems

During consultation, a number of in-vehicle telematics suppliers claimed that their systems met the requirements of the HVDF Legislation. Whilst the study did not undertake an assessment of each offering, it was identified that the claims predominantly revolved around the recording of driver work and rest. However, the functional and business processes were based on the developer's interpretation of the 'electronic environment' of the HVDF Legislation.

Generally, these electronic systems cater for the individual operator's needs but do not allow data to be transferred across operators, have a consistent issuing procedure, provide strong driver authentication or provide a consistent format of information at the roadside. This was not identified as a failing, but rather confirmed that the systems had been designed for a commercial rather than a regulatory use¹.

¹ Importantly, it should be noted that there is currently no interoperability across different electronic systems. Further discussion on interoperability can be found in Section 7.2.1.

3 PHILOSOPHY OF THE SPECIFICATION

The philosophy adopted in developing the specification has been based upon a number of guiding principles:

- The specification for electronic work diaries must meet, at least, the standards of information protection contained within the WWD.
- The specification should be broadly consistent with commercially available electronic record keeping systems².
- The specification should describe the minimum requirements to meet the legal and operational environment of an EWD.
- The specification, where possible, should be performance-based, only being prescriptive in areas to achieve interoperability.
- The specification should allow for both a single and multi-application in-vehicle telematics environment suitable to support both regulatory and commercial use³.
- The specification should be separated into *core* and *application* specific sections. The *core* specifications focus on the requirements of a system that are common across multiple telematics *applications*. The *applications* comprise separate parts for the EWD and for heavy vehicle speed monitoring system specifications.
- The specification should permit Standard Driving Hours, Basic Fatigue Management and Advanced Fatigue Management options and should be flexible to cater for future fatigue management options.

These principles allow innovative solutions developed by the telematics industry to be considered by Authorities for approval.

Security

One of the most important requirements for a regulatory telematics unit is its security, and hence its ability to provide integrity and assurance to governments. Such a feature is critical in other telematics applications and there exist well established principles for security in telematics.

A commonly quoted principle of security solutions is that the 'whole is greater than the sum of the parts'. A whole-of-system approach is necessary for effective security. This principle is applied in the Specified EWD but is compromised in the NTC position. The NTC position would have an EWD with no GPS, no automatic recording of time and position and one that is not tethered to the vehicle. In addition, the NTC position requires a printer.

² Most commercially available telematics systems already utilise GPS technology. See Section 7.2.4 for further discussion.

³ Most commercially available telematics systems operate in a multi application environment. See Section 7.2.2 for further discussion.

The security aspects of the Specified EWD were developed from consideration of two EWD security work packages which were completed in 2009 (Rapp Trans 2009, BenefITS 2009). The first work package determined the broad security architecture necessary for the EWD, and the second work package determined the specific controls necessary for the EWD to offer a level of protection similar to that of the WWD. The recommendations from these investigations have been embedded in the Specified EWD, such that in total, they provide comprehensive and coherent security for the EWD.

A description of the security issues addressed is provided in the box below.

Electronic Work Diary security

1. What security is required within an EWD? The 'protection' offered by security mitigates the threat of an attack. Attacks practically result in the manipulation, corruption or deletion of the data. A four-step 'threat analysis' was followed in order to determine the security architecture suitable for an EWD (Rapp Trans 2009):

1. Determine possible threats - The EWD operating model was determined from the HVDF Legislation. Threats to EWD records were then compiled.
2. Estimate expected losses - Executing one or more of the identified threats would provide the driver with a falsified set of records. This would allow a driver to exceed their regulated working time, causing 'expected losses' of reduced road safety.
3. Define security objectives - EWD security objectives were assumed to be equivalent to those of the WWD.
4. Design countermeasures - The following countermeasures were found to be necessary: use independent trusted third parties, design security from the start, use of certification and use of audit.

2. How strong should the security within the EWD be?

The Austroads Steering Group directed that the security associated with the EWD must provide at least as much protection to data as the controls within the WWD. As the WWD has inherently strong support systems and processes, careful consideration was required to ensure that the EWD could attain an equivalent or higher level of security.

The HVDF Legislation provides a comprehensive list of offences relating to the fatigue of a driver. By examining each offence, it was possible to determine what evidence would be required to support a prosecution. From this, it was then possible to identify threats that would either render this evidence useless or change it so as not to support the offence.

The WWD was found to protect evidence as follows: access to the WWD is controlled, all changes and deletions are recorded, the driver is authenticated, records cannot be repudiated, records are immediately duplicated, and the system is always operable.

Seven equivalent control measures were then determined for the EWD; and from those measures, performance-based EWD control requirements were developed for the system developer and certification authority (BenefITS 2009).

Comparison of the Specified EWD and the NTC positions

As mentioned in Section 1.3, the Specified EWD contains the full details of a device which meets the terms of the Austroads contract with TCA, and includes requirements for a sustainable telematics platform suitable for possible future extended regulatory use. In doing so, some requirements that add greater integrity to the system extend beyond the NTC position.

The Specified EWD fulfils the requirement for an electronic work diary that has the equivalent security, integrity and accuracy requirements expected of a work diary as stated in the HVDF legislation and evidenced in the written work diary and all its processes. The key differences in the requirements of the HVDF Legislation, the NTC position, the Specified EWD and possible future extended regulatory uses are detailed in Table 1. The comparison reveals that the key differences are, in fact, technical and related to the overall integrity of the electronic work diary system. The NTC position and the Specified EWD are in alignment with regards to the roles required in an electronic environment. It is expected that the entities that perform the agreed roles will have strong views on the technical differences. Such technical differences are expected to be addressed and resolved through the upcoming consultation process.

Finally Table 1 also compares the potential uses of the electronic records. The records collected by the work diary can and is being used by drivers, transport operators and the Authorities. How such records can be used in the electronic world, over and above the way they are now, with the WWD, are matters that are unresolved and go beyond this report.

Table 1: Comparison of the system requirements

System aspect		HVDF Legislation	NTC position	Specified EWD	Possible future extended regulatory uses
Roles	EWD Provider	Not required	Required	Required	Required
	DRD Issuer	Not required	Required	Required	Required
	System Manager	Not required	Required	Required	Required
Technical	Interoperability	Not required	Required	Required	Required
	Multi-application environment	Not required	Required	Required	Required
	Paper at roadside	Required	Required	Not required	Not required
System integrity	GPS in in-vehicle unit (IVU)	Not required	Not required	Required	Required
	Automatic capture and populate records	Not required	Not required	Required	Required
	Continuously capture position records	Not required	Not required	Required	Required
	IVU is tethered to vehicle	Silent	Not required	Required	Required
	Tamper monitoring	Required*	Not required	Required	Required
	Time recording resolution	15 minutes	1 minute	1 second	Required
Use of records	Advise drivers how much time remains before a rest break is due, in order to manage compliance.	Not required	Not required	Recommended	Required
	Report breaches and impending breaches to operators, allowing intervention prior to an offence.	Not required	Not required	Not required	Required
	Report instances of gross non-compliance directly to the authority, allowing for intervention by enforcement officers.	Not required	Not required	Not required	Required

* The HVDF legislation requires that drivers comply with the instructions of the Authority. Instructions for using the WWD state that the driver must report all tampering to the Authority within 2 business days.

4 SPECIFICATION FOR THE ELECTRONIC WORK DIARY

This section provides a summary of the Specified EWD including the architecture, roles and interaction between participants, the operation of the EWD and the information recorded by the EWD.

4.1 EWD architecture and stakeholders

The Specified EWD system is shown in Figure 2, and involves the interaction of *up to* seven roles as follows:

1. driver
2. operator
3. Authority
4. enforcement officer
5. EWD (EWD) provider
6. driver recording device (DRD) issuer
7. record keeper.

Whilst not explicitly shown in Figure 2, there is also an overarching System Manager and there may be other third party entities involved, such as an EWD supplier. These roles are necessary for the EWD environment to function properly.

This specification allocates the minimum functions and responsibilities to these roles but does not allocate a particular entity to any particular role. It should also be noted that an entity may perform multiple roles and in doing so takes on the responsibility to perform the functions described under those roles.

The Specified EWD system includes three key pieces hardware:

1. driver recording device (DRD)
2. in-vehicle unit (IVU)
3. printer⁴.

The purpose of the technology and functions of each role is described below in context of the operation of the EWD system.

⁴ Printer is included to align with the HVDF Legislation. The necessity of a printer is discussed in Section 7.2.3.

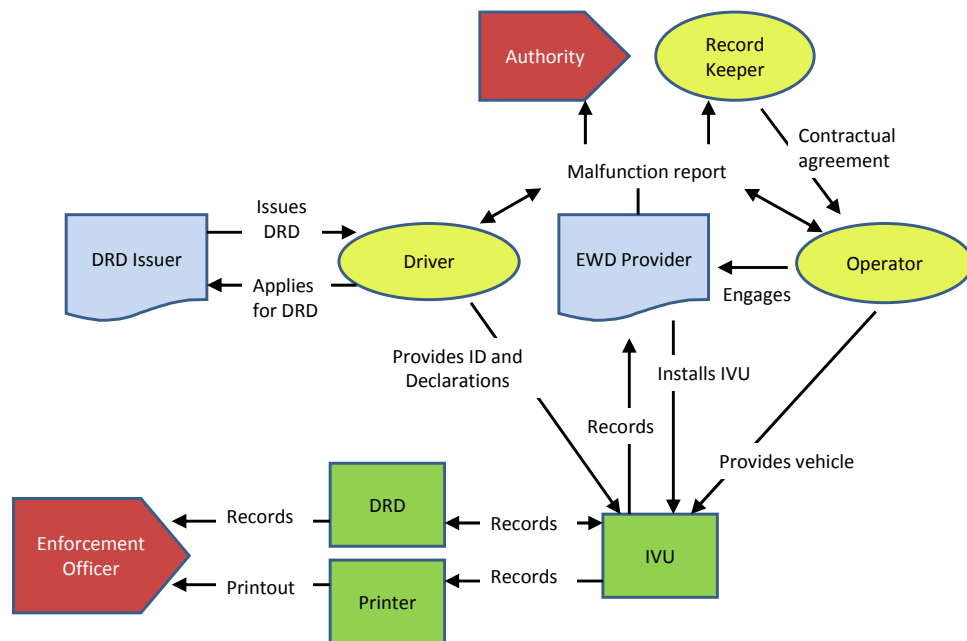


Figure 2: Specified EWD system

4.1.1 Driver Recording Device (DRD)

Similar to the WWD, the DRD stores the electronic records of the driver's work and rest declarations entered into the IVU. The DRD is designed to work with any approved EWD and provides the standardised technology to allow interoperability between operators and enforcement officers.

Physically, the DRD is a secure (can be read from and written to, but does not allow deletions) and driver specific mass storage device based on a Universal Serial Bus (USB) connection⁵ and contains a visible unique identification number. The DRD can store in excess of 12 months of EWD records resulting from normal operation.

4.1.2 In-Vehicle Unit (IVU)

The IVU processes the driver's work and rest declarations. The IVU may automatically populate information to assist the driver in their declarations (i.e. time and location) but is not required to do so⁶. All information must be confirmed by the driver before it is stored. Where the driver disagrees with the automatically populated information, the driver will be able to manually enter the correct information with all changes recorded by the system. The IVU stores a copy of these electronic records on the DRD and sends the same to the EWD Provider for distribution to the record keeper.

It is important to note that the driver's electronic records, stored on the DRD and sent to the EWD Provider, are identical.

⁵ Numerous DRD options were considered throughout the development of the specification. The mass storage device based on a Universal Serial Bus (USB) connection was considered as it was cost effective, readily available and commonly used, can be made secure and provides an interoperable platform between different EWD systems.

⁶ Discussion about the population of information into records can be found in Section 7.2.5.

4.1.3 Printer

The IVU will need to interface to a printer inside the cabin of the truck⁷. The printer will need to provide a standardised rendered version of the driver's records which can be used by an unequipped enforcement officer at the roadside.

4.1.4 Driver

The driver is responsible for declaring their work and rest changes into the EWD system. Each driver shall have a method of identification and authentication for each type of EWD that they use. The method may vary between types of electronic work diaries but shall at a minimum meet specific government standards for electronic authentication.

The driver is responsible for declaring their details and working state (i.e. work or rest) to the IVU. The declaration of their personnel details such as name, driver's licence number and issuing Jurisdiction will be automatically declared by the method of identification and authentication. The working state must be declared by the driver. Depending on the individual system functionality, the remaining information such as time, location, accreditation number, odometer reading and cumulative work tallies may be manually or automatically populated⁸.

Prior to recording the driver will need to accept the information as their declaration. If the system automatically populates information, the driver shall have the ability to change the information. Details of all changes will be recorded by the system.

4.1.5 Operator

An operator is defined by the HVDF Legislation as a person who is responsible for controlling or directing the operations of the heavy vehicle. In the EWD environment, the operator needs to agree to support the EWD system as many systems need some form of vehicle integration (i.e. power supply, mounting etc). The operator is responsible for engaging the EWD Provider to instrument their heavy vehicle with an IVU. The operator may also engage the EWD Provider to supply the IVU for additional commercial purposes.

4.1.6 Authority

The Authority is responsible for maintaining their adopted version of the Heavy Vehicle Driver Fatigue National Model Legislation. Authorities may perform audits of the EWD records held by a record keeper in the same manner as they do with the WWD.

4.1.7 Enforcement officer

The enforcement officer is responsible for inspecting the driver's EWD records. The enforcement officer, if suitably equipped may ask the driver for their DRD and electronically inspect the records. If the enforcement officer is not suitably equipped, they may ask the driver for a printout of the work and rest records.

⁷ Discussion about the use of a printer is found in Section 7.2.3.

⁸ Automatic and reliable population of data into records can be achieved only if the IVU is tethered to the vehicle. Further discussion is found in Section 7.2.7.

4.1.8 Driver Recording Device (DRD) issuer

The DRD Issuer provides the DRD to the driver. The DRD Issuer is responsible for authenticating the identity of the driver, recording the details of the DRD (unique identification number) against the details of the driver and to ensure that only one DRD is provided to the driver at a time. This is not dissimilar to the approach of providing a WWD to a driver.

4.1.9 Record keeper

General

The record keeper is responsible for maintaining the driver's EWD records as specified in the Heavy Vehicle Driver Fatigue National Model Legislation.

Within the HVDF Legislation, the role of the record keeper is allocated to:

- the employer if the driver is employed and working under Standard Hours
- the driver if the driver is self-employed and working under Standard Hours
- the operator if the driver is working under a Basic Fatigue Management or Advanced Fatigue Management accreditation that was granted in combination with the operator's accreditation.

The record keeper may engage the services of another entity, such as the EWD Provider, to assist in performing the record keeping function. If the record keeper does engage the services of another entity, both the record keeper and the other entity are responsible for the record keeping task.

Employer as the record keeper

An employer is defined by the HVDF Legislation as a person who engages someone else to drive a heavy vehicle under a contract of employment, apprenticeship or training. The Specified EWD system is shown in Figure 3.

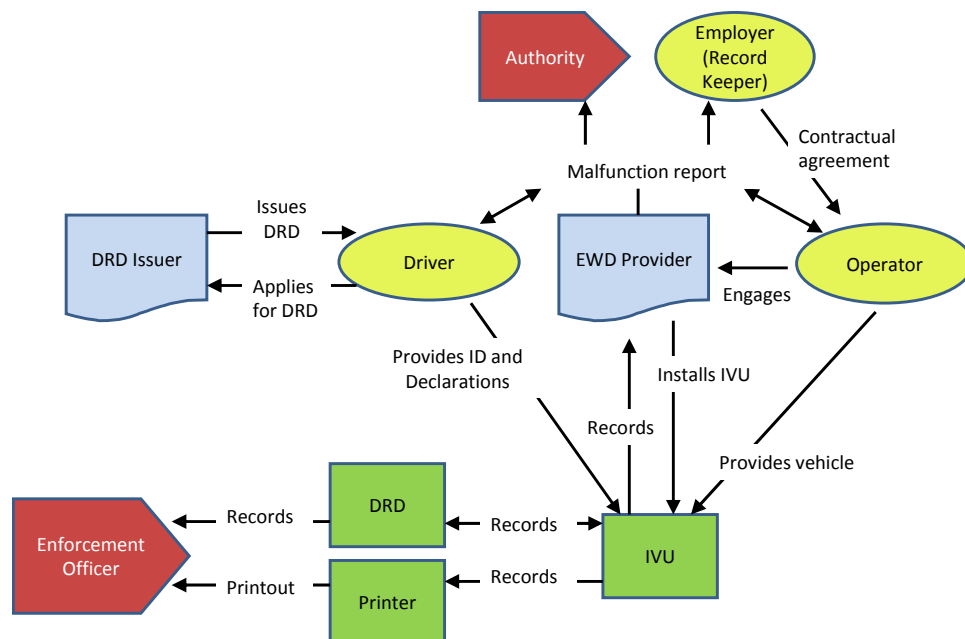


Figure 3: Specified EWD system - employer as the record keeper

Driver (self-employed) as the record keeper

A self-employed driver is defined as a driver who is not an employed driver by a transport operator but is driving a heavy vehicle. In this context, the Specified EWD system is shown in Figure 4. It should be noted that in this context the driver is also performing the function of the operator.

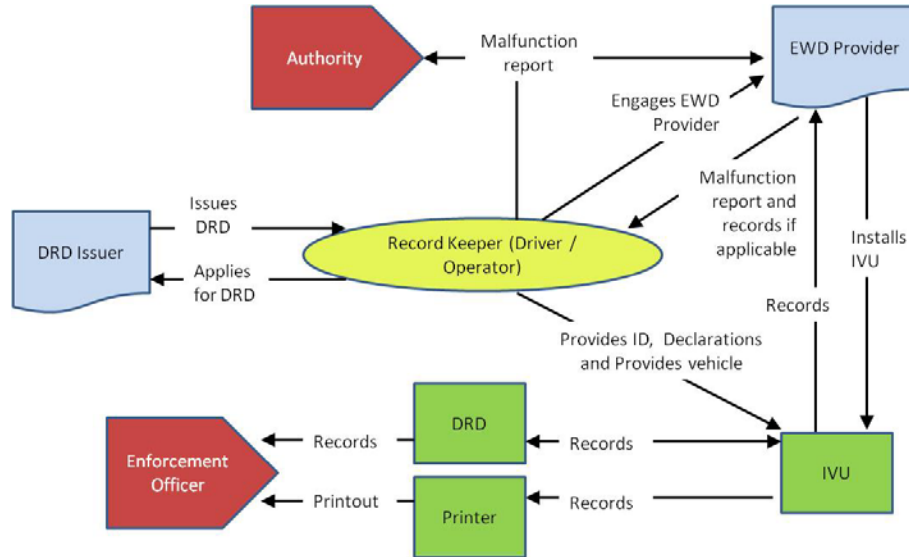


Figure 4: Specified EWD system – driver (self-employed) as record keeper

Operator as the record keeper

An operator is defined by the HVDF Legislation as a person who is responsible for controlling or directing the operations of the heavy vehicle. It should be noted that in this context the operator is also performing the function of the record keeper (Figure 5).

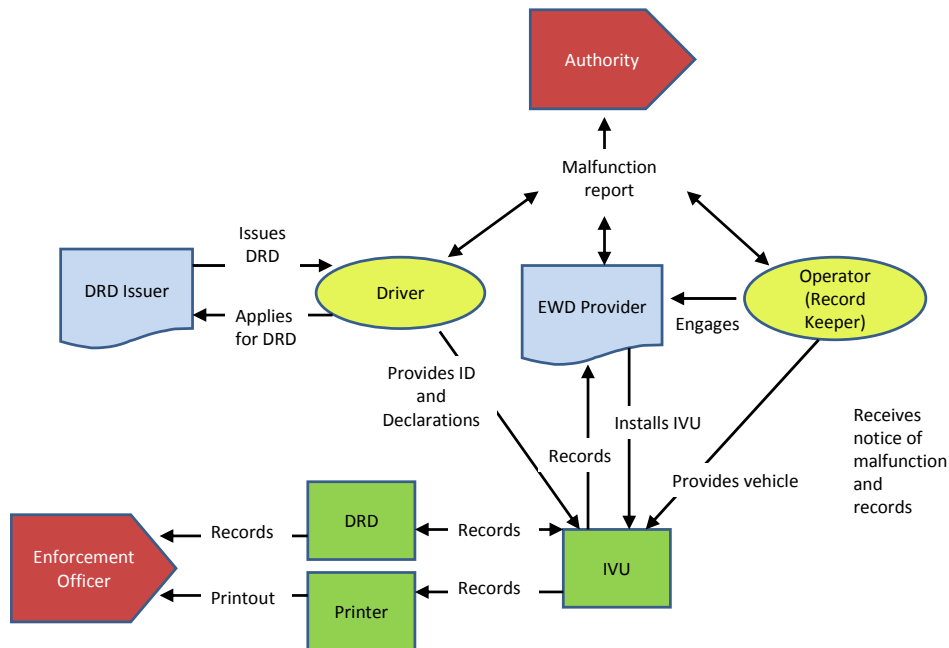


Figure 5: Specified EWD system – operator as the record keeper

4.1.10 EWD Provider

The responsibility of the EWD Provider is to ensure that the EWD system is correctly installed and performs during day to day operation in the same manner as it did when it was approved. The EWD Provider needs to have the operational knowledge of the system to determine its operational state, perform any necessary enhancements and most efficiently deal with malfunctions if they occur. As such, the EWD Provider monitors the operation of the EWD system and reports malfunctions to the driver and operator if required. The EWD Provider may also assist in providing the electronic records to the record keeper. The EWD Provider may be engaged by the record keeper to perform some or the entire record keeping task.

The specification does not limit the number of EWD Providers in the market.

It is anticipated that EWD Providers will offer multiple applications supported from the IVU. Vehicle telematic systems in general use in Australia allow for multi-functional applications. Furthermore, and in some ways more important than any other consideration is that the key reason operators are adopting such systems is to collect data once but use it for many company operational purposes. The EWD Provider is responsible to ensure that the multiple applications operate properly, and not adversely impacting each other. It is envisaged that the EWD systems will require updating from time to time to improve functionality, fix software 'bugs' or update the protection from electronic threats such as software viruses.

The need for an on-going EWD Provider, as opposed to one that only installs the EWD system in the first instance was a consideration in developing the specification. Whilst stand-alone telematic applications still exist, they are becoming less common due to the development and implementation costs associated with making a fully secure and locked down system. This approach also inhibits the ability for the system to be modified in the future which is inconsistent with Australian in-vehicle telematics systems and the philosophy of the specification.

As such, whilst the Specified EWD system is open to the submission for approval of a 'fully secure, locked down and single purpose EWD' potentially not warranting the need for the day to day operational monitoring of a EWD Provider, the Specified EWD system assumes the need for a EWD Provider.

4.1.11 System Manager

The function of the System Manager was an important consideration during the development of the specification.

In contrast to the single WWD, it is expected that there will be a number of EWD Providers supplying electronic work diaries. As the specification is performance-based, it is also expected that each EWD Provider will have a unique solution and offering. The specification permits EWD Providers to combine commercial services with the EWD system and as such, it is expected that EWD Providers will update their offerings from time to time.

The HVDF Legislation requires that each new 'variation' to an EWD be approved by the Authority prior to it being recognised as an EWD. To cope with the number of different EWD submissions and stream variation approvals required, the EWD necessitates the functional role of a System Manager.

The responsibility of the System Manager is to technically assess whether the EWD systems offered by EWD Providers meet the performance-based specification (i.e. are initially approved) and continue to meet their purpose after upgrades and changes are made (i.e. ongoing approval) and provide this advice to the Authority. The System Manager is required to do this assessment consistently across approvals and assist applicants where information or interpretation is required.

The System Manager may also be engaged by the Authority to audit the EWD Provider's EWD systems for operation and provide assurance that the EWD system continues to operate as it was initially approved.

The System Manager also performs the functions of custodian of the performance-based specification EWD system. This task involves modifying or updating the specification to reflect changes in HVDF Legislation or the operational environment.

4.2 EWD operation

This section presents the main operational elements of the Specified EWD environment.

4.2.1 An EWD is approved, it incorporates an IVU and the ability to insert a DRD

The EWD Provider seeks approval from the Authority (or Fatigue Advisory Panel) for the EWD which incorporates the IVU, the ability to insert and record to a DRD and the ability to electronically transmit the records to the record keeper. The Authority in considering the application is likely to engage the System Manager for technical assistance in the assessment task.

The performance-based specification contains requirements around the robustness and suitability of the IVU to meet applicable Australian Standards for heavy vehicle operational environments.

The specification requires that the IVU will be safely and securely installed in the heavy vehicle. In accordance with the HVDF Legislation, the specification requires the EWD to report whether it is, or is not functioning properly to the driver of the heavy vehicle. This includes whether when the IVU or EWD Providers' system is malfunctioning, there has been unauthorised access or tampering.

The electronic records declared and stored by the IVU must be authenticated, have integrity and be secure from interception or corruption.

4.2.2 An IVU is installed in the heavy vehicle

After engagement by the operator, the EWD Provider installs and maintains the approved IVU in a heavy vehicle. This requires the participation of the operator as controller or owner of the heavy vehicle to support an EWD system.

If the record keeper is the employer of the driver, a commercial arrangement may be required between the operator and the record keeper to report and fix malfunctioning electronic work diaries. Under the HVDF Legislation, the record keeper is responsible to ensure the EWD is examined and brought into working order. Practically, the record keeper will need to be informed of any malfunction and will need the co-operation of the operator and the EWD Provider to carry out any required repairs.

4.2.3 The driver identification and authentication method for the IVU

Through the operator, the EWD Provider provides the driver with their identification and authentication method for the IVU. The method of identification and authentication may be unique to each EWD Provider but shall meet at least Identity Assurance Level 3 of the Commonwealth Government's National e-Authentication Framework. The method of identification and authentication may be proprietary to the EWD Provider's IVU and only work with IVUs supplied by that EWD Provider for the operator's specific heavy vehicles.

By not prescribing the method of identification and authentication but rather the standard of assurance provided by the method, the performance-based specification allows existing systems to potentially retain the method they currently use to identify and authenticate drivers.

4.2.4 The driver applies for and is issued with a Driver Recording Device (DRD)

To be able to use an EWD, the driver must apply to the DRD Issuer to obtain a DRD. This may be considered as being similar to a driver applying for a WWD at a motor registry office. Before being issued with a DRD, the driver's identity is authenticated by the DRD Issuer using the driver's licence. The DRD Issuer shall have procedures to populate the DRD with the driver's identity and, if appropriate (say upgrading to a new DRD), the last 28 days of the driver's EWD records.

4.2.5 The driver keeps the DRD

The DRD is specific to a driver, and not the heavy vehicle nor the IVU. The DRD travels with the Driver from one equipped IVU heavy vehicle to another. Each approved IVU will be interoperable with the DRD. It is the responsibility of the EWD Provider to ensure this interoperability is maintained in operation, as initially approved by the System Manager. Once the DRD storage is full, the driver returns to the DRD Issuer to acquire a new DRD. The original, now full DRD is retained by the driver.

4.2.6 EWD records

The EWD system comprises two types of driver declared electronic records (see Section 4.3 for details)⁹:

1. Detail record

This electronic record is created upon the first declaration of work for the day and the IVU (i.e. in the case where two IVUs are used in one day, two Detail records will be created – one in each IVU). This electronic record contains information about the driver, driver's base, applicable fatigue management option in the HVDF Legislation and the location and time.

2. Work record

This electronic record is created at every work or rest declaration. This electronic record contains information about the work and rest change that the driver has declared. This includes the time, location, two-up driver identity (if applicable) and cumulative periods of work and rest¹⁰.

⁹ A third type of record which contains position data from a GPS receiver, is required by the Austroads Specification. Discussion on this requirement is found in Section 7.2.4.

¹⁰ This information is further discussed in Section 7.2.5.

Information within the Detail or Work records may be automatically populated by the IVU. For example, a GPS receiver may be used to automatically generate the location and time of the declaration. Where this functionality is employed, the automatically populated information must be confirmed by the driver prior to recording. Where the driver does not agree with the information, the driver may declare the correct information. The detail of all changes will be recorded including the automatically generated information.

4.2.7 The driver is aided by the EWD which creates electronic records of work and rest (declared by driver)

At commencement of work, the driver uses their identification and authentication method to identify themselves to the IVU. Given this is the first declaration for the IVU it would create a Detail record. This should be considered as the commencement of a new 'session'. The 'session' would end when the Driver elects to remove (i.e. ejects) the DRD from the IVU.

The electronic records (i.e. Detail and Work records) declared by the driver during the 'session' are stored in the IVU.

EWD Providers may have different ways of copying EWD electronic records from the IVU to the DRD. For example, one EWD Provider may instantaneously copy EWD electronic records onto the DRD, this would necessitate the DRD being inserted into the IVU at 'session' commencement. Alternatively, another may prefer to copy the records onto the DRD at the end of the 'session', when the driver elects to remove (i.e. eject) the DRD from the IVU. As stated in the HVDF Legislation, the driver is responsible for operating the IVU in accordance with the EWD Provider's instructions.

At each change from work to rest and rest to work, the driver uses their identification and authentication method to identify themselves to the IVU, and declares if they are working or resting, creating for each declaration a Work record. For example, if the driver's identification and authentication method consisted of a token and a password, the driver would use the token and password and then declare that they were resting via the IVU – this creates one Work record. When the driver returns from their rest, the driver would use their token and password again and declare that they had commenced working – this would then create another Work record.

It is important to note that the EWD does not automatically create a Work record without the driver's declaration. For example, the movement of the heavy vehicle or the turning off of the ignition does not generate a Work record.

If a driver were to change heavy vehicles, the driver would remove (i.e. 'eject') their DRD from the first heavy vehicle IVU and insert it into the second heavy vehicle IVU. If the second heavy vehicle has an IVU supplied by a different EWD Provider, the driver would use their DRD with the new EWD Provider's identification and authentication method to declare their Detail record (first) and then subsequently rest and work via the Work record.

4.2.8 Two-up driver situation (corroboration declared by second driver)

If the EWD system is to be used in a two-up driving arrangement, the second driver is required to use their identification and authentication method to verify the declared electronic records of the first driver (i.e. Detail and Work records). The EWD system will prompt the second driver to corroborate this work and rest change of the first driver by using their identification and authentication method. This is similar to the signature that the second driver provides in the WWD.

4.2.9 Monitoring of IVU

The role of the EWD Provider is to ensure that the IVU performs during day to day operation in the same manner as it did when it was approved. The EWD Provider monitors the IVU via a number of means including receiving the EWD records. The EWD Provider determines the IVU operational state, performs any necessary enhancements and most efficiently deals with malfunctions when they occur.

The EWD Provider reports malfunctions to the driver and operator (as appropriate)¹¹. The EWD Provider also ensures the EWD records are provided to the record keeper (where the record keeper is not the driver).

The operator shall work closely with the EWD Provider to permit the prompt repair and rectification of any malfunction with a heavy vehicle IVU.

4.2.10 The driver's records are available to the Authority and enforcement officer

To inspect a driver's records at the roadside, the enforcement officer can either ask the driver for their DRD or a printout of the driving records.

If an enforcement officer requests the DRD from the driver, the driver removes (i.e. 'ejects') their DRD from the IVU and hands it to the enforcement officer. This is not dissimilar to the way a WWD is provided to the enforcement officer.

The enforcement officer inspects the driver's EWD records by inserting the DRD into the Authority provided remote data terminal (i.e. laptop, PDA or similar) to determine the compliance of the driver's records against the applicable fatigue management option in the HVDF Legislation.

If an enforcement officer requests a printout of the records, the driver will select the period of records requested by the enforcement officer, print and sign the page. The officer will then inspect the records in a similar manner to that of the WWD.

It is important to note that the EWD, like the WWD, does not determine the compliance of the driver. Compliance is determined by the enforcement officer through assessment of the records (either on the DRD or printout) with the relevant regulations.

The Authority would also have access to a driver's electronic records through inspection of the records held by the record keeper. A similar electronic assessment process as per the roadside would be followed.

4.2.11 The records are available to the driver and the record keeper

The EWD records declared by the driver (i.e. Detail and Work records) are provided to the driver and record keeper. The driver retains the DRD which stores the EWD records. The record keeper (if not the driver) is provided the EWD records via the EWD Provider.

¹¹ Reporting of IVU malfunction and tampering is discussed in Section 7.2.8.

4.3 EWD information recorded

The EWD provides the information as required by the HVDF Legislation. As described in section 4.3.6, the EWD system comprises two types of electronic records, namely Detail records and Work records. These are detailed within Table 2 and Table 3 respectively¹².

Table 2: EWD record - Detail record

Name	Generated	Notes
Date	Manually by driver or automatically by IVU	This may be entered by the driver or automatically populated by IVU
Time		
IVU ID	By IVU automatically	This information contains the identification of the recording IVU and is automatically populated by the IVU for each record.
Record number		
EWD Functional and Technical Specification Version Number		
Driver's licence number	By driver via identification and authentication method	This information would be automatically populated within the record by the IVU upon successful authentication of the driver. The information may be contained within the identification and authentication method or contained within the IVU or a combination of both.
Driver's licence issuing Jurisdiction		
Driver's name		
Driver's work and rest scheme (STD, BFM, AFM)		
Accreditation number (BFM and AFM only)		
Driver's base location		
Driver's record location		
Location	Manually by driver or automatically by IVU	
Comment text	Manually by driver declaration	

¹² Details of the third type of record (location record) specified in the Austroads Specification are presented in Section 7.2.6.

Table 3: EWD electronic record - Work record

Name	Generated	Notes
Date	Manually by driver or automatically by IVU	This may be entered by the driver or automatically populated by IVU
Time		
IVU ID	By IVU automatically	This information contains the identification of the recording IVU and is automatically populated by the IVU for each record.
Record Number		
EWD Functional and Technical Specification Version Number		
Driver's Licence Number	By driver via identification and authentication method	This information would be automatically populated within the record by the IVU upon successful authentication of the driver. The information may be contained within the identification and authentication method or contained within the IVU or a combination of both.
Driver's Licence Issuing Jurisdiction		
Driver's name		
Work/Rest status	Manually declared by driver	
Work time or Rest time spent since the last Work/Rest change	By IVU automatically	The IVU maintains a cumulative work and rest time per day and records this information within each record.
Odometer reading at the Work/Rest change	Manually by driver or automatically by IVU	
Registration number of the heavy vehicle		
Registration Jurisdiction of the heavy vehicle		
Two-up arrangement status	By driver manual declaration	
The other Driver's name	By other (second) driver via identification and authentication method	
Other driver's licence number		
Other driver's work diary number		
Jurisdiction that issued other driver's work diary		
Location	Manually by driver or automatically by IVU	
Cumulative daily Work time	By IVU automatically	
Cumulative daily Rest time		
Comment text	By Driver manual declaration	

5 EQUIVALENCE BETWEEN WWD AND EWD

This section examines the equivalence between the WWD and the Specified EWD. Equivalence is examined across three specific areas, namely technical, operational, and stakeholder. Finally commentary is made regarding the overall level of equivalence.

The term 'equivalence', has been adopted, rather than 'the same' because it is recognised that moving from a paper to electronic environment will not be 'the same'. Indeed it is impossible to envisage how one could 'replicate' the WWD operation in the EWD environment. Rather it will be equivalent, that is, *'equal or interchangeable in value, quantity, significance'*, and *'having the same or a similar effect or meaning'*.

5.1 Technical equivalence

The technical environment in which the WWD operates is well documented and understood. The technology of the WWD comprises a WWD (i.e. a book) and a pen used by the driver. The EWD technical environment can be thought of conceptually with the WWD replaced by the DRD and the pen replaced by the ability of the driver to input electronically; that is through the IVU.

From a regulatory perspective, the work diary's primary purpose is to allow the Authority to determine if the driver has worked within their allowable limits. If they have not, then the work diary must provide the Authority with sufficient evidence about the non-compliance. Thus, from an Authority's perspective of equivalence, the driver's records contained within an EWD should be able to be used as evidence with the same confidence as the WWD.¹³

From a transport industry perspective, the work diary's primary purpose is to record the work and rest of the driver for roadside enforcement and to provide information to assist with operational decisions to maintain compliant behaviour. The work diary must be portable and follow the driver into whichever vehicle he or she is working in.

5.2 Operational equivalence

5.2.1 General

This section deals with the area of operational equivalence between the WWD and Specified EWD. This is addressed in two ways, namely the overall business process and its individual features.

5.2.2 Business process

Figure 6 presents the key operations in the WWD business process:

1. A single standard WWD is approved and produced.
2. The driver applies and pays for the WWD.
3. The WWD is issued to the driver by the Authority.
4. The driver completes the WWD which records their identification, work and rest (each page in the WWD is for one day and is in triplicate).

¹³ While the WWD features many control measures, the diary permits the driver to enter their own records without any verification of such declarations. The implications of this are presented in Section 7.2.5.

5. The driver keeps one copy.
6. A second copy is given to the record keeper.
7. A third copy is available to the Authority through the enforcement officer.

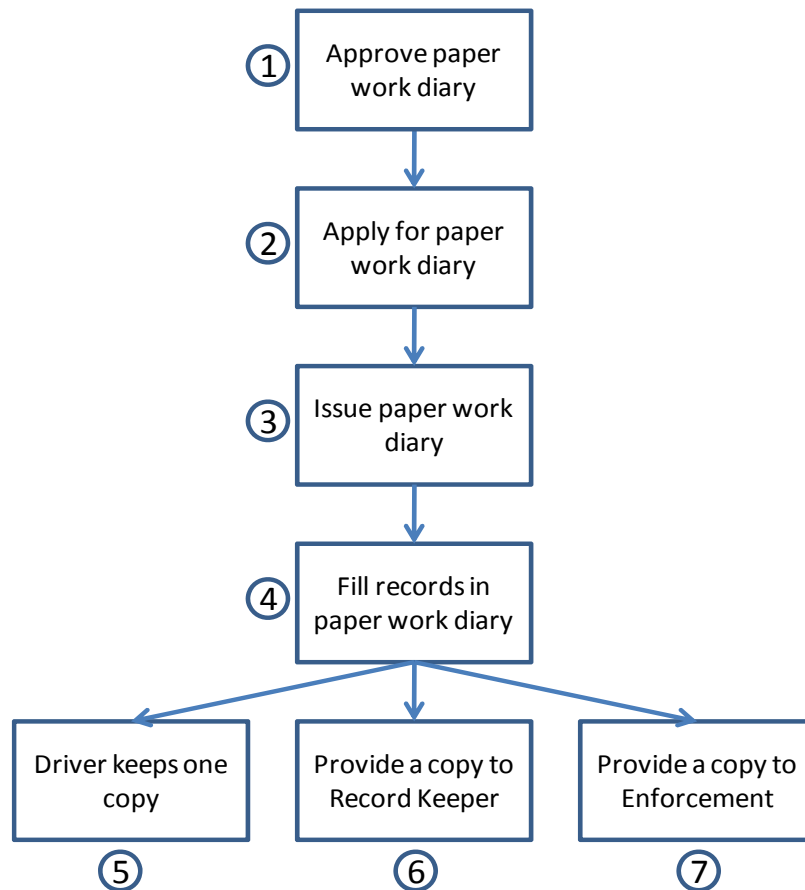


Figure 6: WWD business process

Figure 7 presents the key operations in the Specified EWD business process (numbers link with Figure 7):

1. An EWD is approved; it incorporates an IVU which communicates to the EWD Provider and the ability to insert a DRD.
2. The driver applies for a DRD, and the IVU is installed in the heavy vehicle.
3. The DRD is issued to the driver.
4. EWD records (i.e. Detail and Work records) declared by the driver are stored in the IVU. These EWD records are also copied to the DRD.
5. The driver keeps the DRD which contains EWD records.
6. The EWD records are provided to the record keeper.
7. The EWD records are available to the enforcement officer.
8. The EWD electronic records are available to the operator (subject to record keeper arrangements).

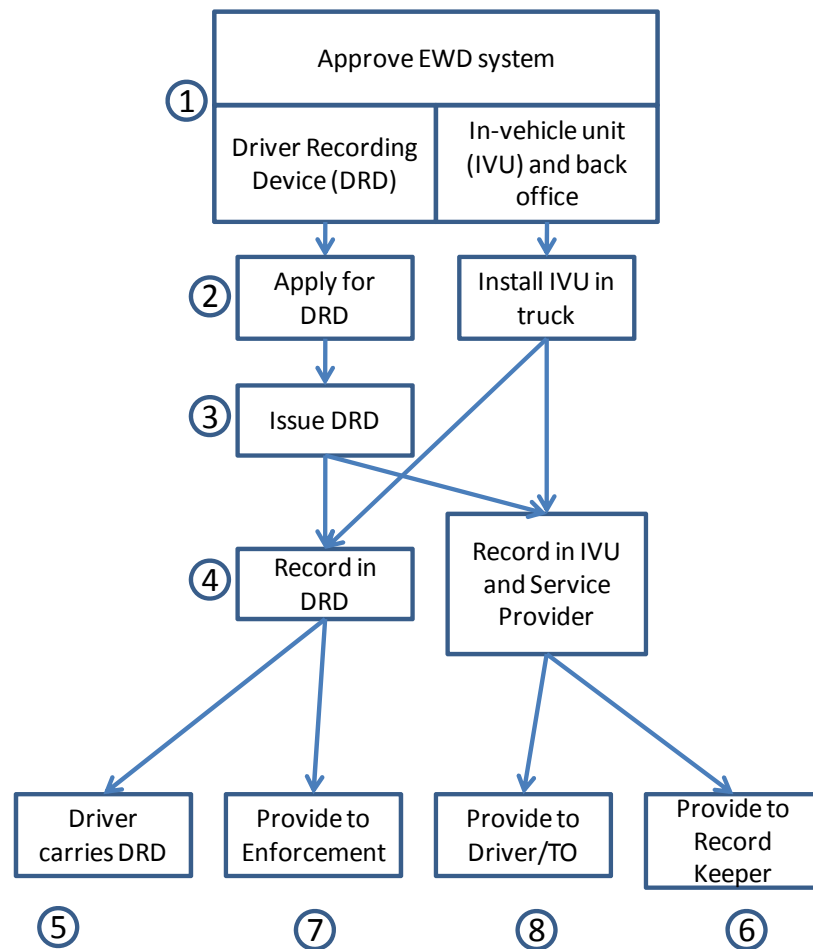


Figure 7: Specified EWD business system

Figure 6 and Figure 7 along with their accompanying descriptions illustrates that the overall business process and flow of information in the WWD and the Specified EWD system approaches are similar.

5.2.3 Features

It is the individual features between the WWD and the Specified EWD that ultimately address the issue of operational equivalence.

This section is not intended to be an exhaustive list of all the features and their comparative equivalence between the WWD and the Specified EWD. Rather a number of 'cases' are used to illustrate the different aspects of equivalence between the WWD and the Specified EWD.

In assessing the issue of feature equivalence the features are categorised into the following 'levels of equivalence':

- *Equal* – the WWD and EWD approaches are essentially the same.
- *WWD equivalent* – interchangeable in significance, with the WWD being more robust, secure or efficient compared to the Specified EWD.
- *EWD equivalent* – interchangeable in significance, with the WWD being less robust, secure or efficient compared to the Specified EWD.

- *Not equivalent* – present in the Specified EWD, but not present or not having a similar effect or meaning in the WWD.

Table 4 provides a number of feature ‘cases’ to illustrate the different levels of equivalence between the WWD and the Specified EWD. In developing the specification, it was observed that most of the WWD and the Specified EWD operational features were equivalent. It was interesting to note that in a number of features the WWD ‘whilst equivalent’ were more robust, secure or efficient compared to the EWD.

Example: Recording of time

A significant feature that is not equivalent between the WWD and the Specified EWD is the recording of time.

The WWD is designed to only allow a driver to declare time in 15 minute increments. The WWD was designed in this manner to simplify the task for the driver when recording and calculating work and rest time. The driver must round work time up to the nearest 15 minutes whilst rounding rest time down to the nearest 15 minutes. Practically, the driver makes these declarations and ensures that their total work and rest time during the day adds up to the total time worked and rested.

For example, a driver may drive for 5 hours and 6 minutes and then rest for 31 minutes. The driver will correctly declare they have worked for 5 hours and 15 minutes and rested for 30 minutes. However, during the next work period, the ‘unaccounted’ 8 minutes (i.e. rounding of 9 minutes up to 5 hours and 15 minutes of work and rounding down 1 minute from 30 minutes of rest) will most likely be soaked up in the next period of work time. If this does not occur, the accumulation of work and rest time rounding will eventually create an implausible situation where there appears to be a greater number of hours in the day than what is possible.

In the electronic environment, the driver may be aided by the electronic equipment to calculate their work and rest. This reduces the need to round the work and rest time to facilitate the ease of recording work and rest time. Further, as most electronic work diaries will make use of some sort of automatic data capture, (most likely the time of the work or rest declaration), it is impractical to round work and rest to 15 minute increments.

In light of these points, the Specified EWD records work and rest to a resolution of at least one minute. That is, time may be recorded to a resolution of a minute or finer (i.e. 1 second).

It is important to note that the measurement of time and the application of tolerances for compliance assessment should be regarded as two separate activities.

Table 4: WWD and the Specified EWD feature 'case' equivalencies

Feature	Written Work Diary	EWD	Level of Equivalence
Diary allocation and portability	- WWD only available from Authority - WWD number linked to driver's identity - One operational WWD per driver - WWD is portable and able to easily follow the driver	- DRD only available from DRD Issuer - DRD identifier linked directly to driver through driver's license number - One operational DRD per driver - DRD is portable and able to easily follow the driver	Equal
Driver declares work and rest	- Declaration made by driver - If driver does not declare, no record is made.	- Work record – declared by driver only - If driver does not declare no record is made - Automatic data capture of time and location is possible but not mandated - Driver permitted to qualify the time and location data	- EWD equivalent - Work record is created at every work or rest declaration. This electronic record contains information about the work and rest periods that the driver has declared. This Work record also contains time and location data that may be automatically populated from the IVU. The driver is permitted to qualify the time and location data with information they believe to be more accurate or indeed make any comment they see fit and necessary.
Driver transfers records to record keeper	Driver physically provides a copy of records to record keeper	EWD Provider provides records to record keeper	- EWD equivalent - The HVDF Legislation requires that records are provided electronically to the record keeper. This requirement prevents the driver from physically providing the records to the record keeper. To ensure this process occurs, where the record keeper is not the driver, all records are provided through the EWD Provider and then onto the record keeper.
Driver authentication of records	Each WWD page is signed by the driver authenticating the records (i.e. biometric information)	The EWD level of authentication is performance based with prescribed assurance level (i.e. Commonwealth's National e-Authentication Framework Identity Assurance Level 3)	- WWD equivalent - The driver's signature is a strong method of authentication as it utilises the author's biometric information to generate the signature. Whilst not equivalent to a biometric standard of authentication, the EWD requires the EWD Provider to provide a method of identification and authentication to the driver.
Records cannot be changed	- Tampering is visible - Pages can be forensically checked - Records are in triplicate	- Use of digital signatures to show author and evidence of change - There is a known set of approved digital signatures - EWD Provider backup and archiving	EWD equivalent
Records are duplicated	WWD provides for immediate duplication of pages, resulting in the original plus two copies	- EWD records are initially stored in IVU and then copied to DRD - EWD records from IVU are sent to EWD Provider	EWD equivalent

Feature	Written Work Diary	EWD	Level of Equivalence
System is always operational	The WWD is always functional	- DRD may fail - IVU maintained and checked for malfunction or tampering by EWD Provider and driver	- WWD equivalent - Apart from the pen, the WWD may be considered as always being operational. No electronic equipment can be guaranteed to always operate and as such, there is no exact electronic equivalent.
Measurement of Time	Measurement of time in the WWD is at 15 minute periods	Measurement of time in the Specified EWD is a resolution of at least one minute periods	- Not Equivalent - It is not feasible to adopt a measure of time different to that of standard electronic measurement. Therefore measurement of time and the application of tolerances for compliance assessment will need to be resolved.
Comments / self declaration	- Driver can make declaration - Driver declares date/time and location as known	- Driver can make declaration - Driver can declare the date/time and location as known or IVU generated date/time and location	Equal
Standard format for records	The WWD has a prescribed format. This format makes it possible for all stakeholders to review records	The DRD and the printout have a prescribed format. This format makes it possible for all stakeholders to review records.	EWD equivalent
Interoperable system	WWD travels with the driver	DRD travels with the driver	Equal

5.3 Stakeholder equivalence

5.3.1 WWD environment

In the WWD environment, all key functions are effectively performed by the Authority and the driver (i.e. user of the system). This is depicted in Figure 8. The driver applies to the Authority for a WWD. During the application process, the driver provides the Authority with proof of their identity and the WWD that is being replaced. The driver pays the Authority and is issued with the WWD.

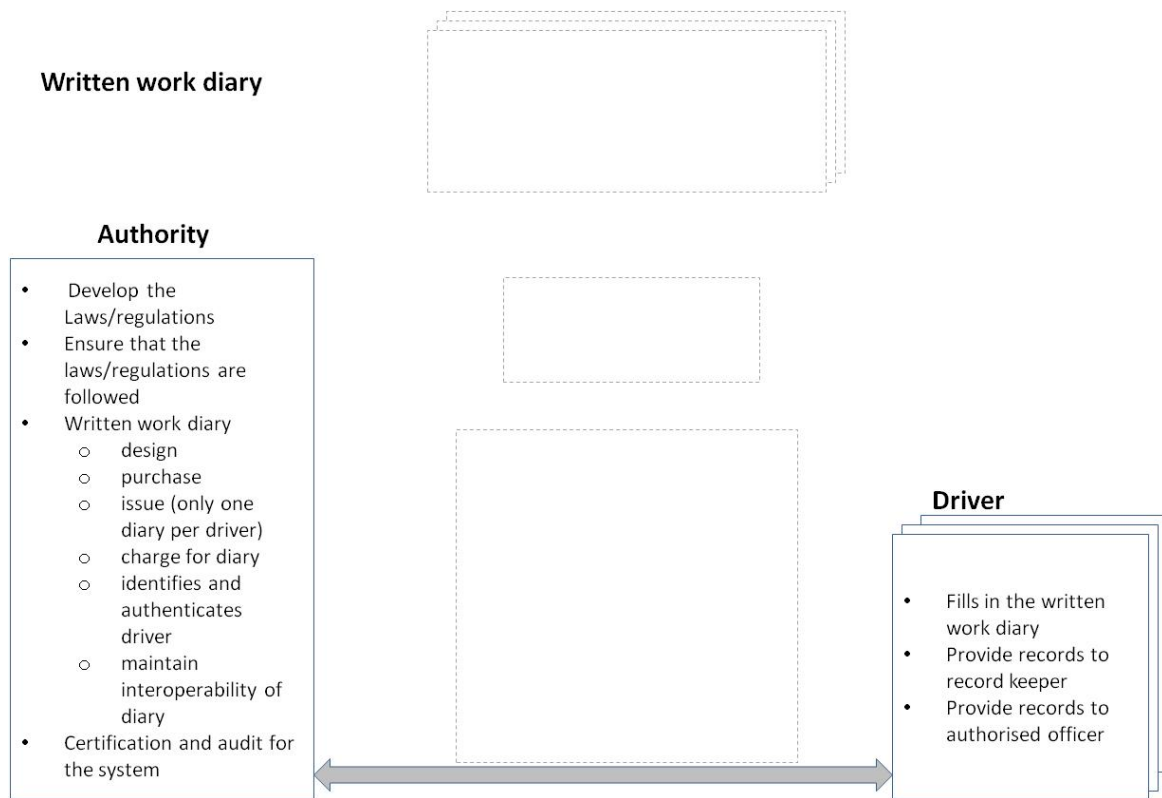


Figure 8: Key stakeholders in the WWD environment

To use the WWD, the driver fills in their identification details and information about their heavy vehicle. At each work and rest change, the driver records the time and location of the stop. At the end of the working day, the driver tallies the total work and rest on that day and signs the WWD page as a true and correct copy of the day's events. The driver is responsible for delivering a copy of the page to their record keeper and carrying the WWD with them whilst they are working. At the roadside, a driver may be required to present their WWD.

The Authority develops the laws and regulations surrounding the WWD and deters non-compliance with these laws through roadside enforcement. The Authority maintains the WWD design, organises its printing and issues the WWD through its offices. The Authority manages the process that ensures only the right driver obtains the WWD and that there is only one WWD per driver in operation at one time. In this context the Authority is regarded as the System Manager.

5.3.2 Specified EWD environment

In the EWD environment, while the functions remain largely the same as in the WWD environment, a greater number of functional roles emerge. This is depicted in Figure 9.

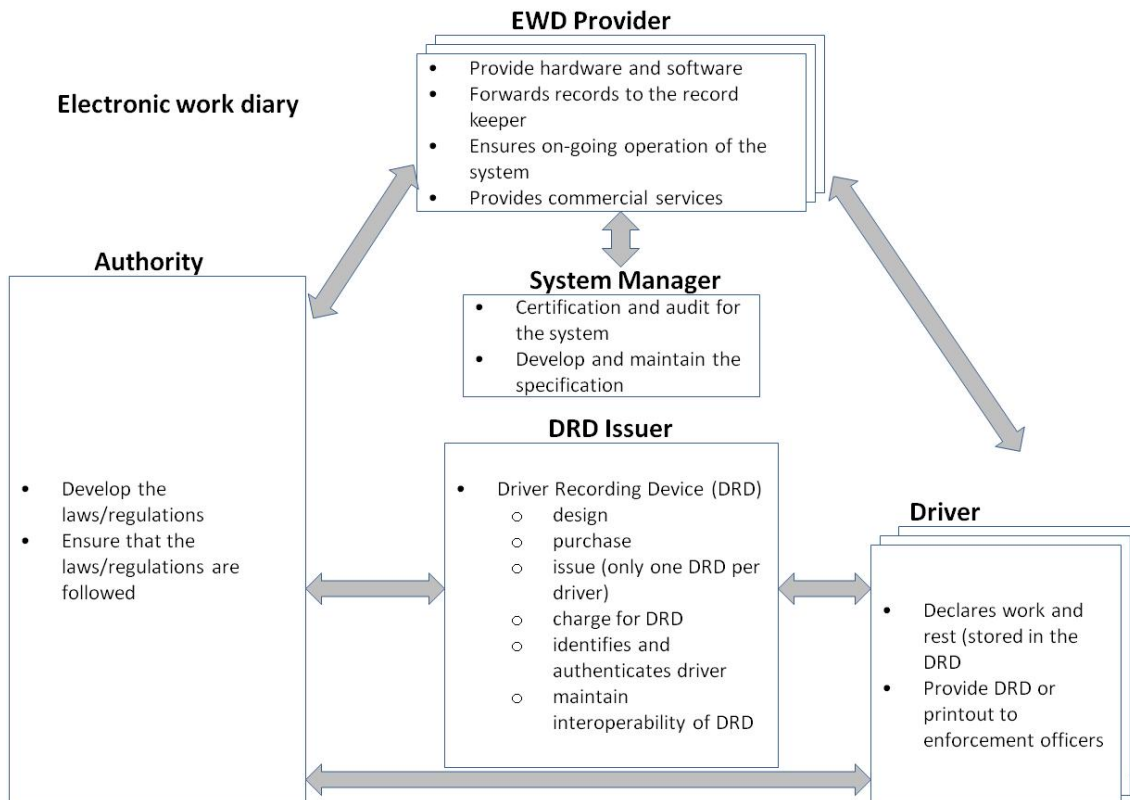


Figure 9: Key stakeholders in the Specified EWD environment

In the Specified EWD environment, the Authority retains the role of developing the laws and regulations and deterrence of non-compliance through enforcement officer roadside inspections.

In moving from the WWD to the EWD environment, there is a significant functional role of ensuring the approved installation and on-going operation of the EWD. For the WWD, the primary responsibility for its day to day functional role lies with the driver. Assuming the driver can interpret and complete the WWD, it is easy to identify that the WWD is 'operational' and not 'malfunctioning'.

For the EWD, the driver is responsible for the records they declare and for being aware of the necessary driver operational responsibilities (e.g. identification and authentication procedures). However, it is unreasonable to expect the driver to be solely responsible for detecting EWD problems or malfunctions. Similarly the operator is not expected to have the necessary skills or training to detect and rectify all EWD malfunctions.

To facilitate the correct installation and monitoring of on-going operation, the Specified EWD system incorporates the role of a EWD Provider. The EWD Provider is the technical expert of their system and is responsible for its installation, maintenance and as necessary upgrade. The EWD Provider is responsible for receiving the data generated from their operator's IVU and transmitting the electronic records to the record keeper. The EWD Provider is also responsible for providing the driver with an identification and authentication method that works with their IVU. This is used by the driver each time they wish to declare a work and rest change.

Before using an EWD, the driver will need to be issued with a DRD by the DRD Issuer. The DRD stores the driver's EWD records and is portable across IVUs. The DRD Issuer is responsible for verifying the driver's identity and ensuring that only one DRD is issued to each driver. The DRD Issuer is also responsible to maintain the interoperability of the DRDs used by drivers.

The driver is responsible for using the identification and authentication method supplied by the EWD Provider, and for using the DRD and IVU to declare their work and rest changes. The driver is also responsible supplying enforcement officers with the DRD at the roadside upon request.

In the electronic environment, a number of different electronic systems may be proposed for approval, each designed and implemented in a different way. These differences necessitate not only an approval process but also an on-going audit process to ensure that the EWD system continues to operate as was originally approved. Further, it is expected that on-going maintenance of the specification and operational environment will be required. To achieve these tasks, a System Manager (i.e. manager the EWD system) is required to perform these functions.

5.4 Overall equivalence

In developing the specification, it was observed that the WWD's and the Specified EWD's technical and business processes were similar. In moving to EWD, the functions already performed in the WWD, required new roles to be created. At the same time, some functions in the Specified EWD are simply not found in the WWD or achieved through a different manner. Importantly, the specification makes no recommendation on actual entities to fulfil the identified roles, nor if some roles can be performed by the same entity. For example:

- EWD Provider – this role requires the technical expertise to install and rectify any malfunctions with the EWD. Can this role be performed by operators or does this need to be an independent third party?
- Driver Recording Device (DRD) Issuer – this role requires the ability to identify and authenticate users of the DRD devices, issue DRDs and provide this information to an Authority. Can this role be performed by an operator, independent third party or is it best allocated to the Authority?
- System Manager – the System Manager will require the technical expertise to assess and approve the technical submission from the EWD Provider. Is this a single organisation or an approved list of approval organisations?

In a number of features the WWD 'whilst equivalent' was more robust, secure or efficient compared to the Specified EWD. Indeed, what appears at first to be a simple book requiring a pen for completion, has, in fact, a sophisticated and secure operating environment that needs to be replicated in the EWD environment.

The following features are 'not equivalent' between the WWD and the Specified EWD:

- Measurement of time in the WWD and the Specified EWD is at 15 minute and at least one minute periods respectively.
- The Specified EWD may utilise the automatic population of information to assist the driver with their declaration¹⁴. The driver is required to confirm all information and may change any information he/she feels inaccurate but all details of changes are required to be recorded.

¹⁴ The Austroads Specification recommends the automatic population of records. Further discussion is presented in Section 7.2.5.

Systems which incorporate automatically populated information from the IVU provide an independent observation which significantly increases confidence in the system as a whole.

6 SPECIFICATION FOR HEAVY VEHICLE SPEED MONITORING

It is important to note that public policy development for continuous in-vehicle speed monitoring is immature and as such, the performance-based specification's focus is predominately on current use. This revolves around the generation and provision of heavy vehicle speed records to the operator. This section provides a summary of the specified heavy vehicle speed monitoring system highlighting the architecture and stakeholder, its operation and information recorded.

6.1 Speed monitoring architecture and stakeholders

The specified system is depicted in Figure 10 and involves three 'players', namely the driver, operator and EWD Provider*. Whilst not explicitly shown in Figure 10, there is also an overarching System Manager.

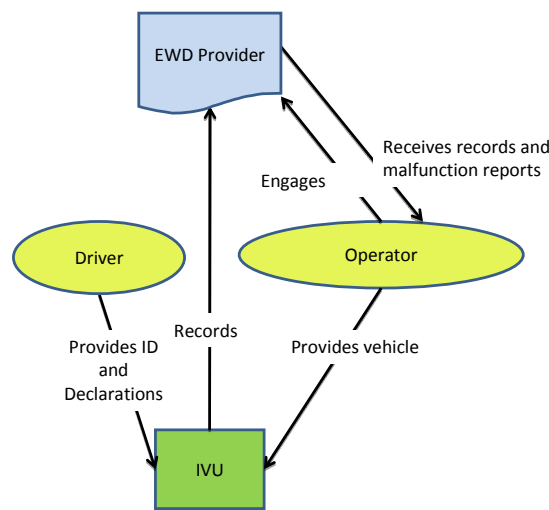


Figure 10: Speed monitoring system

The heavy vehicle speed monitoring system centres on the IVU. The IVU generates vehicle speed periodically whilst the vehicle is turned-on and moving. Vehicle speed is generated independently by the IVU's GNSS receiver. The functions of the stakeholder 'players' in the speed monitoring system are similar to those described earlier for the EWD.

The driver provides their identification to the system at commencement of a 'session' using the identification and authentication method provided by the EWD Provider, through the operator. When the heavy vehicle is turned off, the system will automatically close the 'session'. Each time the heavy vehicle is turned on, the driver is required to identify and authenticate themselves.

6.2 Speed monitoring operation

6.2.1 Speed monitoring system is approved

The EWD Provider seeks approval of the heavy vehicle speed monitoring system which includes the IVU and their back office system, through the System Manager. The specification contains requirements around the robustness and suitability of the IVU for its environment.

* In the context of heavy vehicle speed monitoring the EWD Provider may provide EWD and speed services but for the context of this document the term EWD provider is used.

The IVU will be electrically and physically tethered to the heavy vehicle in a secure manner. There are requirements to detect malfunction or access by unauthorised personnel. The electronic records declared or generated and stored by the IVU must be authenticated, have integrity and be secure from interception or corruption.

The IVU must perform its function within the applicable accuracy standards for GNSS systems and mobile – based communications. Similarly, the EWD Provider must have information security and data access controls for the information they receive, store and forward to the operator.

6.2.2 Speed monitoring system is installed in the heavy vehicle

The EWD Provider installs and maintains the approved IVU into a heavy vehicle. This requires the participation of the operator as controller and or owner of the heavy vehicle to wish to support the heavy vehicle speed monitoring system.

6.3 Driver identification and authentication

Through the operator, the EWD Provider provides the driver (i.e. driver specific) with their identification and authentication method for the IVU. The method of identification and authentication may be unique to each EWD Provider but shall meet the Identity Assurance Level 3 of the Commonwealth Government's National e-Authentication Framework. The method of identification and authentication may be proprietary to the EWD Provider's IVU and only work with IVUs supplied by that EWD Provider.

6.3.1 Speed monitoring system electronic records

The heavy vehicle speed monitoring system electronically generates a Speed record (see section 6.4 for detail). This electronic record is generated periodically by the IVU (i.e. its GNSS capability) when the heavy vehicle is moving. The electronic record contains accurate time and location data¹⁵.

6.3.2 Speed monitoring system automatically generates Speed records

At commencement of work, the driver uses their identification and authentication method to declare themselves to the IVU. Speed records are generated automatically during the 'session' and also stored in the IVU. The driver is permitted to qualify and make comment as they see fit and necessary.

6.3.3 The electronic records are available to the operator

Speed records generated by the IVU are sent to the EWD Provider. The EWD Provider transmits the Speed records to the operator.

¹⁵ This requirement necessitates GNSS functionality in an electronic device that is tethered to the vehicle. Note that the Minimum Specification for EWD does not require GNSS functionality nor tethering to the vehicle. The implications of this are discussed in Section 7.2.4.

6.3.4 Monitoring of IVU

The EWD Provider is responsible to ensure that the IVU performs during day to day operation in the same manner as it did when it was approved. The EWD Provider monitors the IVU via a number of means including receiving the Speed records. The EWD Provider determines the IVU operational state, performs any necessary enhancements and most efficiently deals with malfunctions when they occur.

The EWD Provider reports malfunctions or potential tampering to the operator¹⁶. The operator shall work closely with the EWD Provider to permit the prompt repair and rectification of any malfunction with the IVU.

6.4 Speed monitoring information recorded

The Speed monitoring information required for the specified heavy vehicle speed monitoring system is detailed in Table 5.

Table 5: Speed monitoring information

Content	Generated
Date*	By IVU, automatically
Time*	By IVU, automatically
IVU ID	By IVU, automatically
Record Number	By IVU, automatically
Driver's Licence Number	By Driver, via identification and authentication method
Driver's Licence Issuing Jurisdiction	By Driver, via identification and authentication method
Driver's name	By Driver, via identification and authentication method
Vehicle Speed*	By IVU, automatically
Location (Latitude and Longitude)*	By IVU, automatically

* Date, time, speed and location are generated by the IVU.

¹⁶ Reporting of malfunction and tampering are discussed in Section 7.2.8.

7 UNRESOLVED ISSUES

The Specified Electronic Work Diary Specification (TCA 2009b) proposed a number of technical features which are considered essential for an EWD and heavy vehicle speed monitoring system. These features extend beyond the NTC position that corresponds to a performance equivalent to the written work diary. These features include a requirement for GPS as well as for requirements for a sustainable telematics platform suitable for possible future regulatory use.

These additional features are now discussed in three sub-sections focusing on (i) the roles required in the EWD system (ii) the technical issues and (iii) potential future regulatory uses. These features comprise the unresolved issues that are being taken into the public consultation process.

7.1 Stakeholder issues

In the WWD environment, key functions are effectively performed by the driver, Authority and record keeper. The Specified EWD and heavy vehicle speed monitoring environment necessitates a greater number of roles. Some stakeholder entities are obvious, such as 'driver' and 'operator', however, others need to be progressed and assigned.

Three new roles have been identified and discussed previously in Section 5.3. These roles are; (i) the EWD Provider, (ii) the DRD Issuer and (iii) the System Manager. These roles are common to both the Specified EWD and the NTC's position. Nevertheless, they are unresolved issues for consultation as these roles are not part of the WWD environment.

A further unresolved issue arising out of acceptance and recognition of these three new roles is the question of who will perform these functions. Table 6 details the unresolved stakeholder issues for consultation.

Table 6: Unresolved stakeholder issues

Unresolved issue	Specified EWD	NTC's position
1. EWD Provider	Required	Required
2. DRD Issuer	Required	Required
3. System Manager	Required	Required
4. Who performs these functions?	Unresolved	Unresolved

Neither the NTC's position nor the Specified EWD make any recommendation on actual entities (existing or new) to perform the identified functions, nor if some of those functions could be performed by the same entity. These are policy decisions and comprise:

- **EWD Provider:** the EWD Provider requires the technical expertise to rectify the operation of the system in instances of malfunction. However this same expertise could be used to manipulate or tamper with the system. Can an operator perform this role or does it need to be fulfilled by an independent third party?

- **Driver Recording Device (DRD) Issuer:** the DRD Issuer requires the ability to identify and authenticate drivers and provide them with a DRD. The DRD acts as the single instance of the driver's diary and as such it is critical to the EWD system that the DRD Issuer ensures only one DRD is issued to each driver. It is unresolved if an operator, EWD Provider or Authority should perform this role.
- **System Manager:** the System Manager requires the technical knowledge to assess EWD systems against the requirements contained within the specification. The System Manager must also have systems in place to modify test processes and update the specification if the requirements of an EWD change. Who should perform the role of the System Manager?

In fact, in the WWD environment, similar functions also exist and they have been undertaken by the Authorities. The Authorities are responsible for producing the WWD, identifying and authenticating drivers, providing them with their diaries and ensuring that each driver only has one WWD at a time. The Authority also acts as the System Manager to control any modifications to the WWD.

7.2 Technical issues

There are nine technical issues that remain unresolved. They are detailed in Table 7 and discussed in the sub-sections that follow.

Table 7: Unresolved technical issues

Unresolved issue	Specified EWD	NTC position
1. Interoperability	Achieved via DRD	Achieved via DRD
2. Multiple application environment	Required	EWD and speed monitoring can be stand alone systems
3. Printer	No printer, use DRD (i.e., USB memory stick)	Printer required in addition to DRD
4. Accurate and reliable recoding of location and date/time	Use GPS	Driver records into device, GPS not required
5. Automatic capture and populate records	Required	Not required
6. Location record	Continuously recorded when vehicle in operation	Not required
7. IVU is tethered to vehicle	Required	Not required
8. Tamper monitoring	Required	Not required
9. Time recording resolution	1 second	At least 1 minute

7.2.1 Interoperability

Interoperability between EWD systems

Interoperability exists within the WWD environment because there is only one WWD issued by Authorities that is carried by all drivers and interpreted by all transport operators and enforcement officers.

In the current electronic environment, telematics providers design their systems differently and many commercial systems operate as closed systems. There is currently no interoperability across different commercially available electronic systems.

To use EWD in a regulatory environment, however, interoperability is a necessity. Drivers need to be able to bring their work and rest records across different EWD systems. As such, a Driver Recording Device (DRD) was defined in the specification as a means of enabling interoperability across different EWD systems. The specification defines the DRD as a data storage device with a USB connection. The data formats and protocols of the DRD have also been specified to ensure that consistent records can be transferred between systems.

While it has been argued that the driver recording device is an essential component for the EWD system in order to achieve interoperability across different systems (both transport operators and government), this remains an unresolved issue for consultation and resolution.

Interoperability between WWD and EWD systems

A further interoperability issue is when drivers require access to both their WWD and the EWD. Contract /loan drivers are obvious examples where this is possible. This report does not provide a solution at this stage. It has identified that this is an unresolved issue to be added to the list of matters to be resolved.

7.2.2 Multiple application environment

In industry, it is common to see telematics technology supporting multiple software applications. For example, the one in-vehicle telematics unit may incorporate engine monitoring, route guidance, cargo tracking, speed and load temperature monitoring applications.

It is envisaged that regulators will find more uses for telematics in the future and continue to release regulatory applications to improve efficiency and safety in road use. With the increase in regulatory and commercial applications, it will not only be impossible to fit an increasing number of single use telematics boxes within the cabin of a truck, it will also be unsafe for the driver to be trying to operate all of these devices at once.

It is therefore important that a regulatory box that is being specified should be capable of supporting multiple applications. Conceptually, this is illustrated in Figure 11 which depicts different multi-application IVUs.

A regulatory IVU may contain only regulatory telematics applications and would be provided to an operator who was solely interested in compliance.

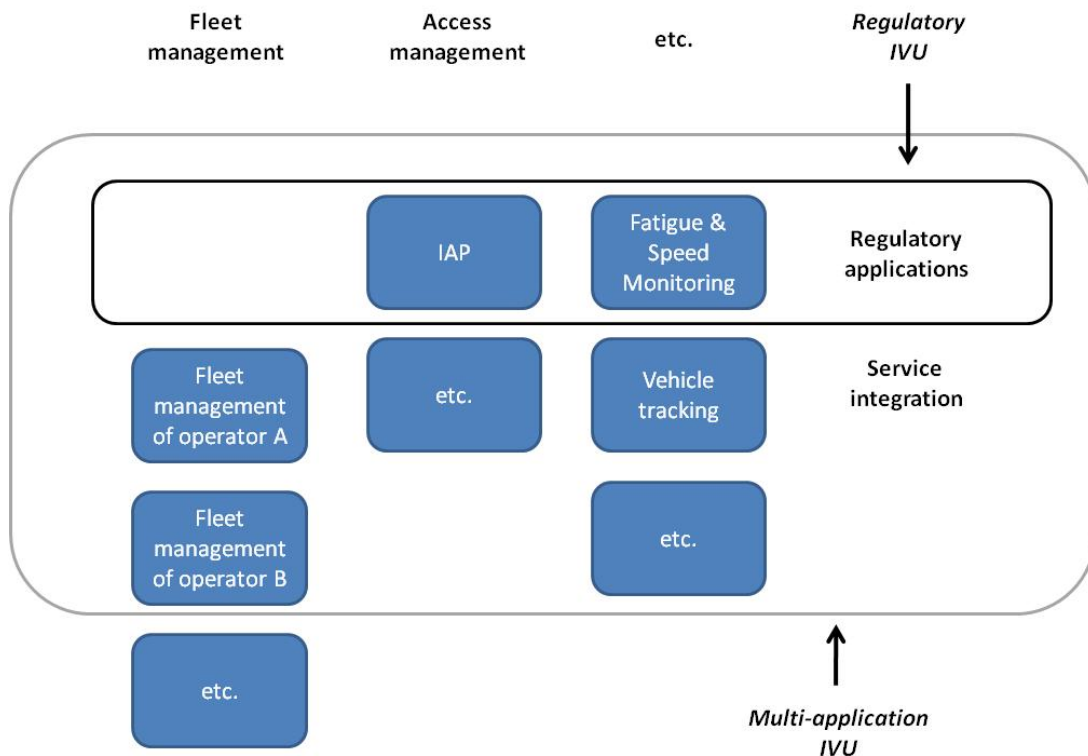


Figure 11: Various IVU configurations

A multi-application Specification should therefore permit the single telematics box to use common information for many different applications. The most significant advantage this provides is the prevention of duplicating sensors and overall processing.

The multi-application Specification also allows for a managed approach to what information the driver receives or is required to input. This has a significant safety benefit for the driver, as they are only interacting with one device rather than many devices which may compete for the driver's attention at the same time.

The concept of a core platform for a multi-application environment for regulatory and commercial use is therefore an unresolved issue for consultation.

7.2.3 Printer

The Specified EWD requires that work and rest records be stored in electronic form in the DRD. Upon a roadside inspection, the enforcement officer will request that the driver provide the DRD, plug the DRD into a laptop or a personal digital assistant (PDA) installed with certain software to check the relevant records and determine compliance.

Current policy does not provide any direction to require additional equipment carried by an enforcement officer. Therefore, in order to provide readable work and rest records at roadside inspections, a printer was added into the specification to provide a printout of the records.

A study was undertaken to investigate the costs of requiring a printer in the EWD system. It was recognised that for compliance checking purposes, a printer will not only impose an upfront hardware cost, but also costs associated with installation, maintenance and on-going printing. The study estimated that a printer will introduce an additional 40% cost to the total EWD system (Austroads 2010). Furthermore, according to the current level of roadside inspection, on average a driver's work diary is checked less than once per year. Considering such significant additional costs and low usage, it is difficult to justify specifying a printer. For these reasons, commercial systems available today do not utilise printers.

While it was strongly recommended not to include a printer in the EWD system, this requirement remains in this specification in order to satisfy the requirements of the HVDF Legislation. It is up to policy makers to decide whether the printer should remain a requirement.

7.2.4 Accurate and reliable recording of location and date/time

The HVDF Legislation requires accurate information to be recorded. In order to capture accurate information (location, date/time), the Specified EWD requires a GPS receiver in the IVU. On the other hand, in order to achieve equivalence to the WWD, GPS is not required by the NTC policy position. One may argue that removing the GPS requirement makes the EWD no different to the WWD in terms of data integrity, because the work and rest information is still declared by the driver. But in so doing, the EWD would be deprived of the accuracy and integrity of an independent sensor.

A guiding principle in the development of this specification was to make the specification broadly consistent with commercially available electronic record keeping systems. In consultation with telematics service providers and transport operators, it was found that most current electronic systems incorporate GPS as a basic component to capture accurate location, time and date information. Excluding the requirement of GPS from the specification does not only contradict the guiding principle, but it also downgrades a regulatory system below current commercial standards.

The issue of GPS in the EWD is a matter for resolution.

7.2.5 Automatic capture and populate records

The weakest link within the WWD system is the declaration of the driver's work and rest information. Compliant drivers will accurately record when and where work and rest interchanges occur. However, in a paper diary, there is little to prevent a driver from falsifying these records to appear to be compliant. Furthermore, it is also difficult for an Authority to detect a well-scripted but falsified record.

Electronic records provide the opportunity for greater integrity because location, date and time components of the driver's declaration can be automatically generated and are protected with sequential numbering and other security features. Automatic record capturing and population are required by the Specified EWD however not supported by the NTC policy position. This is a further issue for resolution.

Back dating of records

In addition to driving, drivers also work on tasks such as loading and unloading vehicles. As these non-driving tasks are also classified as work, they need to be declared as part of the work records in the work diary. The HVDF Legislation requires the driver to declare work at the beginning of the work period. In the WWD environment, drivers are able to back date their work records at a later time because it is the driver who determines when the records are entered into the work diary.

In one case, a driver may start work not knowing whether they have to do work beyond 100 km from their depot. Subsequently, sometime after they have commenced work, they are reassigned to a task that requires a trip greater than 100 km from their depot. Under the HVDF Legislation, they then must immediately fill in their work diary with all prior work from the start of their shift.

As electronic devices record continuously and automatically, in an electronic world, a policy decision is required as to whether or not back dating by drivers should be permitted in the EWD system. It is technically possible to prevent drivers from back dating work records, but in so doing, this may affect the current industry practices and be inconsistent with the HVDF Legislation. Assuming that the decision is likely to be to permit back-dating, policy and technical work-arounds will need to be considered for this to occur in an EWD that continuously and automatically records data. This issue can be further investigated and resolved after an operational pilot.

7.2.6 Location records

The Specified EWD features location records which are automatically generated by the IVU using the GPS capability when the heavy vehicle is turned on. The minimum contents of a location record are shown in Table 8.

Table 8: Contents of location record

Content	Generated	Notes
Date	automatically by IVU	Current date, time and location of the turned – on heavy vehicle where the periodic record was made. This information is generated by the IVU's GNSS capability
Time	automatically by IVU	
IVU ID	automatically by IVU	
Record Number	automatically by IVU	
Location (Latitude and Longitude)	automatically by IVU	

The NTC's position does not require that an EWD features location records. The issue of whether or not the IVU should continuously capture location records will be taken to consultation.

7.2.7 IVU is tethered to vehicle

Tethering of the IVU to the vehicle is a requirement of the Specified EWD, however this is not supported by the NTC policy position. The NTC position therefore allows some portability. It was argued that as a WWD is not tethered to the vehicle, so an equivalent EWD should not be tethered to the vehicle either.

Tethering IVU to the vehicle is a key EWD feature which governs the security around the entire EWD system. As a simple example, if an IVU could be removed from the vehicle without being reported, any records collected by the IVU would not have any evidentiary value as they may not necessarily link to a heavy vehicle.

Nevertheless, tethering IVU to the vehicle remains an unresolved issue and will be taken to consultation for resolution.

7.2.8 *Tamper monitoring*

There is agreement that the EWD shall report if the system is malfunctioning. However an unresolved issue is whether the EWD system should monitor for tampering.

Tamper monitoring is one of the most important features that distinguish a regulatory telematics system to a commercial one. In all regulatory telematics applications, efforts have been made to design systems to be at least tamper evident if not wholly tamper proof.

The NTC's position does not require monitoring of potential tampering events because it was argued that the HVDF Legislation does not require a WWD to monitor tampering events and therefore neither should an EWD system. The Specified EWD requires tamper monitoring and the generation of Alarm records to report potential tampering events (Specification A.20).

While tamper monitoring is an essential feature of any regulatory telematics application (including EWD), it remains an unresolved issue for consultation.

7.2.9 *Time recording resolution*

The WWD is designed to only allow a driver to declare time in 15 minute increments. The driver must round work time up to the nearest 15 minutes whilst rounding rest time down to the nearest 15 minutes. Practically, the driver makes these declarations and ensures that their total work and rest time during the day adds up to a total of 24 hours for each day.

In the electronic environment, time can be recorded to a finer resolution. The NTC's position requires a resolution of at least one minute for the work and rest records. The Specified EWD requires time to be recorded to 1 second. This technical issue remains unresolved.

7.3 Possible future extended regulatory uses

The Specified EWD will provide information as specified in this report. The way this information is used, by the Authorities for a range of future extended regulatory uses is yet to be resolved. Table 9 details the main issues raised. The WWD is fundamentally a single usage instrument. The EWD, like other such electronic systems, has the ability to take collected information and use it in ways for purposes beyond its original intent.

As identified previously, one of the motivational factors of the transport industry in adopting an EWD application has been to streamline and integrate driving, working (not driving) and rest monitoring as part of the entire 'track and trace' solution and use the driver information for company operational purposes. In a similar manner, Authorities may consider alternate and complementary ways or purposes of using EWD information.

Table 9: Possible future extended regulatory uses

Unresolved issue	Specified EWD	NTC position
1. For the driver: Driver warnings, alerts, advisories and assistance	Permitted	Not required
2. For the operator: Use of records for non regulatory purposes by operator	Permitted	Not required
3. For the Authority: Use of records for reporting of non-compliances to Authorities	Unresolved	Not required

A range of other potential uses are as follows:

- Operator
 - Managing customer contracts by provision of heavy vehicle speed compliance reports
 - Improved management of heavy vehicle operations and performance.
- Authorities
 - Potential reporting of gross speeding by exception, directly to the Authority (and/or operator) – there is no regulatory requirement to ‘report’ breaches currently other than that which may be imposed through a court imposed monitoring sanction.
 - The consideration of the monitoring, sanctions, best use and effect resulting from more sophisticated and overt speed monitoring.

The vehicle telematics industry (i.e. EWD Providers) may wish to consider the provision of ‘driver-aids’ and ‘warnings’ and a capacity for to report breaches as part of the Specified EWD and heavy vehicle speed monitoring system¹⁷.

These unresolved issues are also worthy of taking forward to consultation, perhaps not for resolution at this stage, but certainly for discussion as principles and directions going forward for future projects.

¹⁷ There is the opportunity to include such a specification in Part A.8 *Non-regulatory functionality in the IVU*. (See Appendix A, specification A.8)

8 WHAT NEEDS TO HAPPEN NEXT?

The EWD specification will be progressed through the Austroads approval process, and the NTC position paper will be finalised and approved for joint release before the August SCOT meeting. A joint consultative process will then be undertaken. As a result of this consultation, a final position will be reached which can be recommended to Ministers at ATC. The proposed pilot of electronic work diaries (to be led by NSW) will be needed to resolve some key points – particularly relating to the need for a capacity for in-cab printing.

A series of steps are proposed as a setting for going forward. Figure 12 provides a possible roadmap of the next steps depicting the phasing of the operational pilot, arrangements for legacy systems together with the consultation process as well as the process to resolve the unresolved issues.

The roadmap proposes three distinct phases leading to the Specified EWD and heavy vehicle speed monitoring system becoming available to stakeholders following an operational pilot (2010-2012) and a period for the transition of legacy systems.

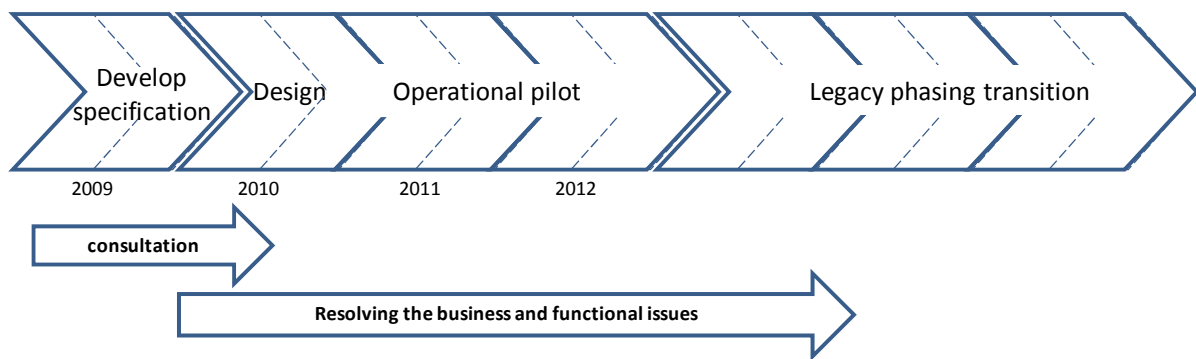


Figure 12: Possible roadmap of the next steps

8.1 Consultation

Austroads seeks for stakeholders to consider the operation of the EWD as described within this document and provide input.

The consultation process will involve:

- presentations and meetings with Authorities,
- presentations and meetings with transport industry groups (and associated Authority), and
- presentations and meetings with telematics industry and developers.

It is anticipated the consultation process will continue until forth quarter 2010, at which time a refined version of the performance-based specification will be delivered.

8.2 Operational pilot

In developing the specification, it was observed that whilst electronic systems for fatigue and heavy vehicle speed monitoring are available and to varying levels appreciated by Authorities and the transport industry, the institutional and business systems environment required to support it in a regulatory context is not as developed. This includes the unresolved issues identified previously.

As such, it is recommended that an operational pilot of the Specified EWD and heavy vehicle speed monitoring systems be completed. This would be the appropriate means for all stakeholders to experience the NTC's position and the Specified EWD in the real world. The operational pilot should not be seen as testing the technology, rather, the business systems, human interaction and institutional processes; that is, the technology's environment of operation.

It is envisaged that the operational pilot would take no less than 18 months and could, subject to Authorities approval interface with the legacy arrangements.

8.3 Dealing with operator legacy electronic systems

Throughout consultation with stakeholders, it was recognised that with the investment made by some operators to electronic systems, consideration should be given to permitting legacy phasing arrangements (i.e. transition), as part of achieving the Specified EWD and heavy vehicle speed monitoring systems. For example, some transport operators operate their own stand alone system without a service provider. In the future, there may need to be consideration for a stand alone system integrated with approved EWD systems, yet managed by the transport operator.

Austrroads is conscious of the investment made by operators seeking to introduce electronic systems to improve compliance. It is acknowledged that an Authority may consider other factors in deciding potential legacy phasing or transitional arrangements to a final EWD system.

The table below summarises the key areas requiring transitional arrangements, and the associated requirements in the specified EWD system from the main report.

Table 10: Key issues for transitional arrangements

Issue	Transitional arrangement	The specified EWD
Recording of work and rest times	Minimum resolution is 15 minutes block as required in the HVDF	Time is recorded in one second resolution
Driver identity and data portability	Physical or electronic (PIN) ID, portability may not be required	driver Recording Device, portability is achieved across all systems
Driver identity and authentication	Unique IDs within a closed system	Specified the Australian Government Standard for identity and e-authentication
Data integrity	Restriction to data alteration	Third party Service Providers maintain high integrity
Roadside data	Printer to be available	Equipped enforcement officers read driver Recording Devices
Enforcement and compliance	Unchanged	Generation of reports to Authorities
Solution	Multiple solutions, non interoperable	Interoperable
Certification	Manager of the system	Manager of the system
Speed monitoring	Speed data is collected	Speed data is collected and provided to transport operators

The Authority will be the approver of the various commercial electronic systems that are presented for approval under the transitional/trial arrangements. A four step approval process is outlined in Figure 13.

1. **Submit application:** applicant submits application to the Authority by presenting a commercial electronic system and filing an application form.
2. **Review application:** the Authority reviews the application against the minimum requirements set out in this section. If any obvious non-compliance is identified, the Authority rejects the application and responds to the applicant with reasons for rejection. If no obvious non-compliance is identified, the application is progressed to a detailed review stage. In a trial period a non-compliant system may be accepted if it has additional features which strengthen its capacity to support fatigue or speed compliance, or which may provide valuable trial lessons.
3. **Detailed review by the Authority:** the Authority reviews the application in detail including technical, operational and legal requirements met by the commercial electronic system.
4. **Authority's decision:** the Authority makes the final decision according to the level of non-compliance and informs the applicant of its decision.

It is envisaged that the Authority will be advised and assisted by the System Manager.

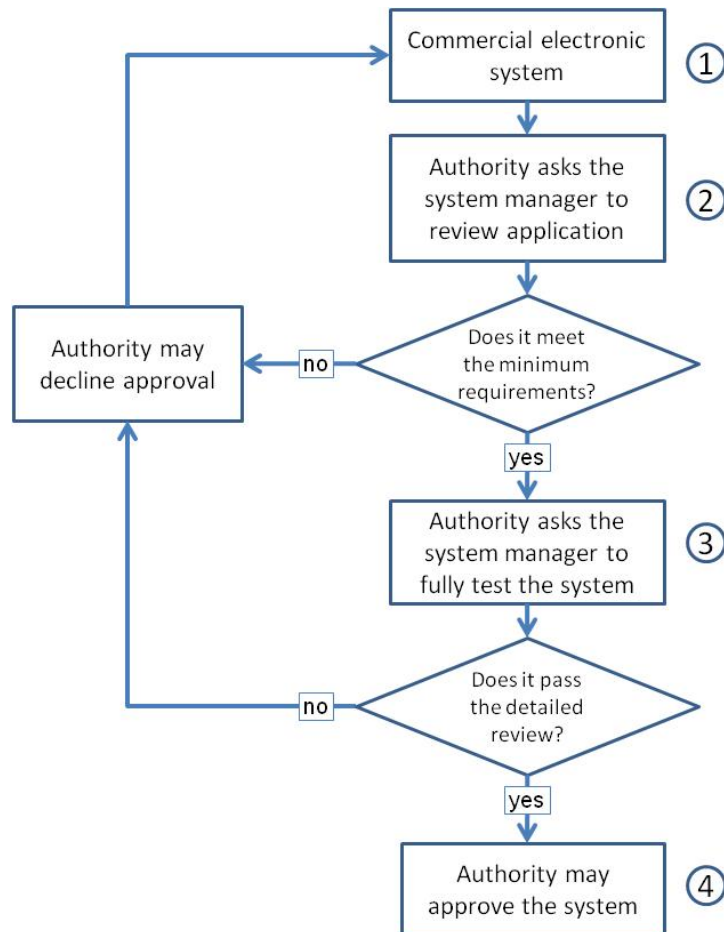


Figure 13: Approval process for transitional arrangement

REFERENCES

- Australian Transport Council 2008, *Joint Communiqué, Australian Transport Council*, 7 November 2008.
- Austroads 2009, *Consultancy Agreement with Austroads Incorporated*, Sydney, NSW, March 2009.
- Austroads 2010, *The Cost of Paper at the Roadside*, Damien Hill and Transport Certification Australia, February 2010.
- BenefITS consulting 2009, *An Analysis of the Controls Necessary to Protect the Evidentiary Quality of Information in Electronic Work Diaries*, Melbourne, Victoria, 9 November 2009.
- Department of Finance and Deregulation 2009, *National e-Authentication Framework*, Commonwealth of Australia, Canberra, ACT, January 2009.
- National Transport Commission 2006a, *Model Legislation – Heavy Vehicle driver Fatigue Regulations 2006*, National Transport Commission, Melbourne, Victoria, 2006.
- National Transport Commission 2006b, *Road Transport Legislation – Compliance and Enforcement Regulations 2006*, National Transport Commission, Melbourne, Victoria, 2006.
- National Transport Commission 2007, *Model Legislation – Heavy Vehicle driver Fatigue Regulations 2007*, National Transport Commission, Melbourne, Victoria, 26 September 2007.
- National Transport Commission 2008a, *Electronic Recordkeeping, Data Security Management*, National Transport Commission, Melbourne, Victoria, July 2008.
- National Transport Commission 2008b, *Electronic Recordkeeping, driver Device Issuance and Control*, National Transport Commission, Melbourne, Victoria, April 2008.
- National Transport Commission 2008c, *Heavy Vehicle driver Fatigue National Model Legislation*, National Transport Commission, Melbourne, Victoria, 25 August 2008.
- National Transport Commission 2008d, *Model Act on Heavy Vehicle Speeding Compliance Regulations 2008*, National Transport Commission, Melbourne, Victoria, 17 July 2008.
- National Transport Commission 2009, *Electronic Systems for Heavy Vehicle driver Fatigue and Speed Compliance: Draft Position Paper*, National Transport Commission, Melbourne, Victoria, July 2009.
- Rapp Trans Group 2009, *Electronic Work Diary - Security Analysis*, Rapp Trans Group, Basel, November 2009.
- Transport Certification Australia 2006, *Intelligent Access Program (IAP) Functional & Technical Specification*, Transport Certification Australia, Melbourne, Victoria, March 2007.
- Transport Certification Australia 2008a, *Australian Requirements for Tachograph Application*, Transport Certification Australia, Melbourne, Victoria, 4 March 2008.
- Transport Certification Australia 2008b, *Australian Specifications for Tachograph Application*, Transport Certification Australia, Melbourne, Victoria, 30 September 2008.
- Transport Certification Australia 2009a, *Fatigue and Speed Management System Requirements (Draft)*, Transport Certification Australia, Melbourne, Victoria, June 2009.
- Transport Certification Australia 2009b, *Electronic Work Diary Specification (Draft)*, Transport Certification Australia, Melbourne, Victoria, November 2009.
- Transport Certification Australia 2009c, *Appendices to the Electronic Work Diary Specification (Draft)*, Transport Certification Australia, Melbourne, Victoria, November 2009.
- Queensland Government 2006, *Queensland Government Authentication Framework – Authentication Concepts, Version 1.0.3*, Queensland Government, Brisbane, Queensland, October 2006.

SPECIFICATION DOCUMENT

The Specification document presents the Specified EWD and a version of an EWD and separate heavy vehicle speed monitoring device that corresponds to the preferred policy position presented in the NTC's position paper. The documents are:

1. Appendix A – Specified EWD.
2. Appendix B – NTC position on the EWD.
3. Appendix C – NTC position on heavy vehicle speed monitoring device.

The NTC positions on EWD and heavy vehicle speed monitoring device are sub-sets of the Specified EWD. According to the NTC's position, a minimum specification for EWD has no GPS in the IVU, the IVU is not tethered to the vehicle, the IVU does not record speed and requires a printer. However for heavy vehicle speed monitoring, the NTC's position is that GPS is necessary.

A discussion on these differences can be found in Section 7 of the report.

The reader is directed to begin by reading the Specification for Electronic Work Diary and Heavy Vehicle Speed Monitoring (Appendix A) as it best informs the reader about the specified fully-functional system. The NTC positions in Appendices B and C are best understood once the reader is aware of the specified all-encompassing solution.

The specifications are laid out as follows:

- Part A – Specification for In-Vehicle Unit (IVU)
- Part B – Specification for EWD Provider
- Part C – Specification for Self Declaration Input Device (SDID)

The NTC positions in Appendix B and C do not repeat the introductory information contained in the Specified EWD Specification in Appendix A.

The Specified EWD addresses all the unresolved issues in Section 7 of the report.

Part A (the specification for the IVU) is fully detailed as far as possible (given the unresolved issues). In some areas of Part A, the reader will find a shorter specification, because the full requirements have yet to be resolved. However, wherever that occurs in Part A of the specification, reference can be made to the IAP Functional & Technical Specification by way of example.

Part B (the specification for the EWD Provider) is one of the unresolved issues identified for consultation. In some areas of Part B, the reader will find a shorter specification, because the full requirements have yet to be resolved. However, wherever that occurs in Part B of the specification, reference can be made to the IAP Functional & Technical Specification by way of example.

A copy of the IAP Functional & Technical Specification is available from TCA, subject to an NDA, and requests can be made to Mrs Karen Barker at (+61 3) 8601 4675 or email karenb@tca.gov.au.

CORE AND APPLICATION SPECIFICATIONS

The Specified EWD has been designed around the concept of Core and Application specific sections.

The Core specifications focus on the requirements of a system that are common across multiple telematics applications. For example, the specification around the technology to determine the location of the In-Vehicle Unit (IVU) would be considered as a core specification. These would be common to access, fatigue, speed and mass applications.

Application specific specifications focus on the specification requirements of a particular application. For example, the specifications regarding the recording of working hours may only be applicable to some applications. In this example, these specifications would reside within the Fatigue application specification.

Separating the specifications in this manner allows for the incremental addition of further applications by the regulators. The Core requirements are common to all applications. As a new application is offered by the regulator, a new incremental specification will be released. It is envisaged that the new application will draw upon as much of the functionality contained within the core requirements as possible. The additional functionality will be described in the application specific specification and it is hoped that the incremental certification will be minimised in size and cost.

Figure A – 1 conceptually illustrates a number of application specific specifications referencing the same core requirements or core platform.

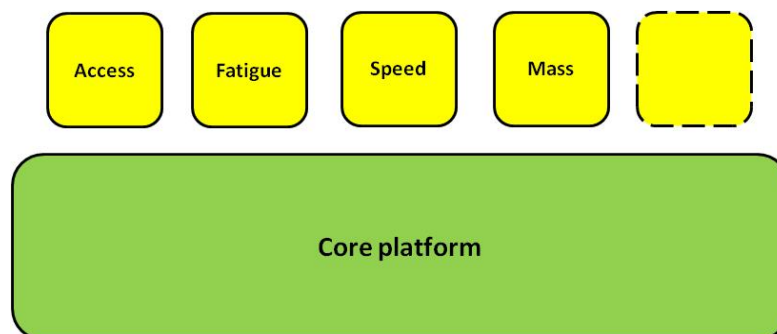


Figure A – 1: Technical architecture of specification

It was also identified that the IAP F&T Specification could be considered as containing two types of specification requirements: those that are common to any regulatory telematics application and those that are unique to the Access application.

Further, it was recognised that as IAP is a functioning and operating regulatory application, the EWD Specification would benefit from specification requirements that have been tested and implemented by telematics providers today. To allow for this, TCA has separated the IAP F&T Specification into Core and Access Application specific specifications and utilised the Core specifications where possible.

Separating the Specifications into Core and Application specific requirements also allows for the concept of a multi-application In-Vehicle Unit (IVU). A multi-application IVU allows for many applications to run concurrently from the one telematics box. With the increasing information provided to the driver, it is important for the driver's safety, to have these managed and delivered from the one device.

APPENDIX A – SPECIFIED EWD

1 CORE SPECIFICATION

The specifications within the next sections are designed to be as informative as possible. Each specification has a preceding commentary which provides the reader with the motivation of why the specification is necessary.

The specifications are contained in the grey boxes. To manage intellectual property concerns, any specification that has been derived from the IAP F&T Specification has been provided in reference and title only. Any specification that has been produced as a result of the Austroads contract is detailed in full.

The Core and Application Specifications have been arranged into the IVU, EWD Provider and SDID sections. Under each of these sections, the specifications have been grouped into logical subjects.

The Specification is numbered to inform the reader as to the section they are referring to. For all specifications, those that start:

- with an A refer to the IVU (i.e. A.X.1.2)
- with a B refer to the EWD Provider (i.e. B.X.1.2)
- with a C refer to the SDID (i.e. C.X.1.2)

If the specification has a second letter reference, this shall refer to:

- the Fatigue Application if it is appended with an F (A.F.1.2)
- the Speed Project if it is appended with an S (A.S.1.2)

Note: Core Specifications do not have a second letter.

The Specification, as described within the Methodology in the Executive Summary utilises the intellectual property contained in the IAP Functional and Technical Specification. Where a specification requirement has been duplicated within this report, the IAP Functional and Technical Specification title is provided with a new reference number in accordance with the format described above.

1.1 Specification for In-Vehicle Unit (IVU)

1.1.1 Physical and environmental characteristics

This section of the Core Specifications deals with the physical and environmental requirements of the In-Vehicle Unit (IVU). It describes the components of the IVU and its physical properties that are considered necessary in a robust and reliable solution.

In-vehicle telematics may be broadly defined as a device within the vehicle that contains both telecommunications and automatic data capture. Considering this, the IVU shall collect, monitor and store accurate positional information and other data relevant to the EWD application and be able to communicate with an EWD Provider.

A.1 In-Vehicle Unit (IVU)*

- A.1.1 The EWD Provider shall provide an In Vehicle Unit (IVU) that collects, monitors and stores Global Positioning System (GPS) and other data and transfers that data via a communications device to the EWD Provider.
- A.1.2 An IVU shall be inclusive of:
 - a. a GPS receiver
 - b. a communications device
 - c. all cabling, connections and fixings.
- A.1.3 Other forms of Global Navigation Satellite System can be proposed and adopted by an EWD Provider subject to the approval of System Manager.
- A.1.4 An IVU shall be robustly connected to the respective prime mover/rigid truck.

A.2 IVU GPS capability*

- A.2.1 The IVU GPS receiver and GPS antenna shall comply with the all relevant requirements from Australian Communications Authority (the Class Licence).

A.3 Documentation (for IVU)*

- A.3.1 The EWD Provider shall document, to the satisfaction of the System Manager, the IVU and all components, cabling and their interfaces.

Traceability of IVUs will be important for an in life service perspective and for an understanding of where records have been generated. As such, each IVU shall be identifiable by carrying a unique identifier.

A.4 IVU identifier*

- A.4.1 Each IVU shall have a unique alphanumeric identifier (IVU ID) that will be used to identify:
 - a. the particular IVU
 - b. data from that IVU, when being processed or stored by the EWD Provider System.
- A.4.2 The IVU ID shall be visibly marked on the outside casing of the unit as well be stored in the non-volatile programmable read-only memory of the IVU.

It is expected that the IVU will be used to collect records which may be used as evidence for a prosecution. As such, it is important that any removal or opening of the IVU by un-authorised personnel is detectable.

A.5 Security*

- A.5.1 The IVU shall be protected to ensure detection of any unauthorised removal or opening of the IVU.

As many applications will require some level of interface with the driver (i.e. in the case of fatigue a driver will need to declare if they are working or resting), the IVU shall be capable of accepting a self declaration from a device connected to the IVU (Self Declaration Input Device or SDID).

* For an example please refer to the IAP Functional & Technical Specification.

A.6 Self Declaration capability*

- A.6.1 The IVU shall be capable of accepting input from a Self Declaration Input Device (SDID) installed by the EWD Provider.

Regulatory telematics applications will involve the IVU being located on or in the heavy vehicle, the hardware should be able to withstand the environmental conditions that may be found within the vehicle.

A.7 Suitability for use in vehicles*

- A.7.1 The EWD Provider shall provide to the System Manager, evidence of compliance from an appropriate body to demonstrate the suitability for use in vehicles for the IVU and all associated components.

It is envisaged that the IVU will provide a platform for EWD functionality and other commercial applications such as engine monitoring, vehicle tracking, route guidance and fleet management services. As such, the IVU shall be permitted to have non-EWD functionality as long as it does not corrupt the functionality of the EWD application.

Many commercial electronic systems currently provide alerts to drivers when they reach their driving time limit. While this is not a required regulatory function, it is obviously an important feature that assists drivers in compliance to their work and rest requirements.

A.8 Non-regulatory functionality in the IVU*

- A.8.1 It shall be permissible, subject to the approval of System Manager for non-regulatory functionality to be accommodated within the IVU.
- A.8.2 The regulatory functionality shall be isolated from any non-regulatory functionality that may be provided by the IVU.
- A.8.3 The EWD Provider shall document, to the satisfaction of the System Manager, any non-regulatory functionality to be provided by the IVU.

1.1.2 Data collection and record generation

The use of GPS or other GNSS systems to calculate position and date and time data removes the need for drivers to manually record this data. This also provides the ability for improved accuracy of location data, especially where a rest break occurs in an area with little or no easily definable features. As such, the IVU shall need and store collect position and time data. Whilst the policy work is not complete on speed monitoring, it is expected that Authorities shall want to be able to monitor the speed of the vehicle and connect this to the driver of the vehicle. As such, the IVU shall monitor the speed of the vehicle at regular intervals.

As the IVU will be used to provide evidentiary level data, the IVU must have a mechanism to infer that the IVU has recorded data correctly.

* For an example please refer to the IAP Functional & Technical Specification.

A.9 Data*

A.9.1 The IVU shall collect the following data:

- a. GPS quality data (refer A.10)
- b. date and time data (refer A.11)
- c. vehicle position data (refer A.12)
- d. vehicle direction of travel data (refer A.13)
- e. vehicle speed data (refer A.14)
- f. Odometer data (refer A.16)
- g. alarm status data (refer A.15)
- h. Self Declaration (SD) data (if applicable) (refer A.17).

A.9.2 The IVU shall process the collected data to produce the following IVU Data Records which are stored for later transmission:

- a. Location Records (refer A.18)
- b. Speed Records (refer A.19)
- c. Alarm Records (refer A.20)
- d. SD Records (refer A.21).

A.10 GPS quality data*

A.10.1 GPS quality shall be measured to the satisfaction of the System Manager.

A.11 Date and time data*

A.11.1 The IVU shall collect and store date and time data in the format defined by the System Manager.

A.11.2 The date and time shall be stored with a resolution of 1 second.

A.11.3 The IVU shall have an internal clock that operates independently of the supporting external power supply.

A.12 Vehicle position data*

A.12.1 The IVU GPS receiver shall determine latitude/longitude position of the vehicle.

A.12.2 The latitude/longitude position calculated by the IVU GPS receiver shall not deviate by more than the standard US Department of Defence Accuracy for the absolute horizontal position Australia wide.

A.13 Vehicle direction of travel data*

A.13.1 The IVU GPS receiver shall determine direction of travel of the vehicle.

A.13.2 The direction of travel determined by the IVU GPS receiver shall not deviate from the actual direction of travel by more than 4 degrees.

A.14 Vehicle speed data*

A.14.1 The GPS reported vehicle speed greater than 60 km/h shall be accurate to within 3.0 km/h for 99.9% of the measurements.

A.15 Alarm status data*

A.15.1 The connection of the IVU to the external power supply shall be monitored and reported upon in accordance with A.20.1a.

* For an example please refer to the IAP Functional & Technical Specification.

- A.15.2 Movement of the vehicle shall be detected and reported upon in accordance with A.20.1b.
- A.15.3 The independent movement features to facilitate the detection of vehicle movement shall be approved by the System Manager.
- A.15.4 The EWD Provider shall document its chosen method of independent movement detection and connection.
- A.15.5 The removal of the IVU from the vehicle shall be monitored and reported upon in accordance with A.20.1c.
- A.15.6 Access to the IVU shall be monitored and reported upon in accordance with A.20.1d.

The odometer reading of the vehicle is expected to be an important source of information. Under the HVDF Legislation, a driver is obligated to record the vehicle odometer reading of the vehicle when they declare a work / rest change. As such, the IVU shall be required to record odometer information.

A.16 Vehicle odometer data

- A.16.1 The IVU shall be able to record the odometer reading at every work/rest change.
- A.16.2 The odometer reading shall be stored to a resolution of 1 km.

As described previously, the driver will need an interface to declare information to the IVU. The information will need to allow for both structured and free text input. The declaration should also be confirmed to the driver.

A.17 Self Declaration (SD) data*

- A.17.1 The IVU shall have the capability of receiving, confirming receipt of and storing SD data only from a Self Declaration Input Device (SDID) connected to it.

Location and Speed Records should be generated at regular intervals, whilst Alarm and SD Records should be generated when an alarm or self declaration event occurs.

A.18 Location Records

- A.18.1 The IVU shall generate Location Records from the data collected by the IVU, and store them.
- A.18.2 Location Records shall be continuously generated and stored at periodic time intervals when the vehicle is in operation.
- A.18.3 A vehicle shall be considered to be in operation when the IVU's supporting external power supply is connected to the IVU and the ignition status is on.
- A.18.4 A Location Record shall consist of at least the following data:
 - a. record number
 - b. date / time of generation (UTC format)
 - c. vehicle position
 - d. direction of travel
 - e. GPS quality
 - f. status of other independent movement sensors.

* For an example please refer to the IAP Functional & Technical Specification.

A.19 Speed Records*

A.19.1 The IVU shall be capable of determining a measurement of the speed of the vehicle.

A.19.2 The IVU shall, while the vehicle is in operation, generate Speed Record at periodic time intervals.

A.19.3 A Speed Record shall consist of at least the following data:

- a. record number
- b. date / time of generation (UTC format)
- c. vehicle position
- d. vehicle speed
- e. GPS quality

A.20 Alarm Records*

A.20.1 The IVU shall generate and store Alarm Records for the followings:

- a. power reading
- b. movement without power
- c. removal of IVU
- d. access to any part of IVU

A.20.2 An Alarm Record shall consist of at least the following data:

- a. record number
- b. date / time of generation (UTC format)
- c. the event that triggered the generation of the Alarm Record as per A.20.1.

A.21 SD Records*

A.21.1 The IVU shall generate SD Records from the SD data entered.

As IVU Data Records may be used as evidence, it is important that they are associated with a unique record number. This record number allows each record to be distinguished and more importantly, allows for missing or out of sequence records to be easily identified.

A.22 Record numbering*

A.22.1 Location, Alarm and SD Records shall be assigned record numbers from the one record numbering sequence, with consecutive and increasing record numbers assigned to successive IVU Data Records in order of generation.

A.22.2 Speed Records shall be assigned record numbers from a separate numbering sequence, with consecutive and increasing record numbers assigned to successive Speed Records in order of generation.

1.1.3 Storage, display and transfer

The IVU will need to be able to store the records prior to sending them on to the EWD Provider. The IVU shall have sufficient memory to accommodate Location, Speed, Alarm and SD Records.

* For an example please refer to the IAP Functional & Technical Specification.

Note: it is recommended the IVU is designed to be capable of expanding the storage for additional applications.

A.23 IVU Data Record storage capability*

A.23.1 The IVU shall be capable of storing at least 20,000 Location, Alarm and SD Records (combined) and at least 200,000 Speed Records.

It is expected that the vehicle will be powered down occasionally for routine maintenance. In these instances the IVU will need to retain all data.

A.24 IVU external power supply failure/shutdown*

A.24.1 In the event that the external power supply supporting the IVU fails or shuts down, the IVU shall be capable of retaining stored data and monitoring the status of the movement sensors for a period defined by the System Manager.

Data collected by the IVU should not be able to be manipulated by any person, device or system. Security and confidentiality of data stored within the IVU shall be maintained at all times.

A.25 Data security and confidentiality measures*

A.25.1 It shall not be possible for collected or stored data or software memory within the IVU to be accessible or capable of being manipulated by any person, device or system (including the SDID), other than that authorised by the EWD Provider.

To ensure that the IVU meets the reporting requirements, the IVU shall be capable of communicating in the vehicle's chosen area of operation and maintain standards of data security, privacy and integrity.

A.26 IVU communication capability*

A.26.1 The IVU shall be capable of communicating with the EWD Provider from at least the areas nominated by the EWD Provider.

A.26.2 The channel for the transmission of IVU Data Records to the EWD Provider shall be secure and guarantee standards for privacy and data integrity to the level defined by the System Manager.

A.27 Transfer of data from IVU to EWD Provider*

A.27.1 The transfer of stored data from the IVU to the EWD Provider shall be performed at least once every 24 hours provided that the IVU is in the communication coverage area offered by the EWD Provider and the vehicle is in operation.

A.27.2 IVU Data Records stored in the IVU shall only be deleted after such data is transferred from the IVU and successful receipt is confirmed by the EWD Provider.

A.28 IVU Data Records*

A.28.1 IVU Data Records shall be transferred from the IVU to the EWD Provider.

A.28.2 Every transfer shall include framing data that identifies its sequential order, IVU ID, version number of IVU component plus software and ability to decode or decompress data.

A.29 Integrity and origin of IVU Data Records*

A.29.1 The numbering shall be sequential.

* For an example please refer to the IAP Functional & Technical Specification.

- A.29.2 Each transfer shall contain error detection and error correction coding that operates successfully.
- A.29.3 Each transfer shall support a form of data authentication (i.e. some form of message authentication only known and accessible to the EWD Provider), subject to the approval of the System Manager, that can prove the origin and integrity of the IVU Data Records.
- A.29.4 The EWD Provider shall document, to the satisfaction of the System Manager, the transfer authentication mechanism.

A.30 Integrity and origin of SD Data*

- A.30.1 Similar to the integrity of the communication channel between the IVU and the EWD Provider, the SDID should ensure that there is integrity, confidentiality and authenticity of the driver declaration data.

A.31 IVU approval

- A.31.1 To facilitate IVU approval testing, multiple IVUs shall be provided to the System Manager.

1.2 Specification for EWD Provider

1.2.1 IVU Installation, operation and maintenance

To ensure that the equipment is fit for use as it is specified, all IVUs will need to be approved by the System Manager prior to installation within a vehicle.

B.1 Type-approved IVUs*

Critical to the successful recording the location, speed and driver declaration data is the correct installation and ongoing operation and maintenance of the IVU. The IVU will periodically need maintenance (such as replacement of batteries). Further, dependent on the implementation, the in-operation of the device in the presence of a fault may not be obvious. As the most knowledgeable entity with the device, the EWD Provider shall be responsible for the correct installation and commissioning of the IVU within the vehicle.

The EWD Provider will also be responsible for the continued operation of the IVU and its on-going maintenance.

B.2 Installation of IVUs*

B.3 Operation of IVUs*

B.4 Maintenance of IVUs*

B.5 Documentation (managing IVUs)*

1.2.2 Self Declaration Input Device (SDID) installation, use and maintenance

Similar to the IVU, the EWD Provider shall be responsible for the installation, operation and maintenance of the SDID.

B.6 Installation of SDIDs*

B.7 Use of SDIDs*

B.8 Maintenance and replacement of SDIDs*

B.9 Documentation (managing SDIDs)*

1.2.3 EWD Provider system

One of the decisions a EWD Provider will need to make in designing their system is the number of vehicles that the system must be capable of monitoring. The IT resource and infrastructure, software and personnel required to monitor this number of vehicles will then be matched to the design.

As such EWD Providers System will be certified on the basis of it being able to cater for a set number of vehicles. For example, a EWD Provider may apply for certification of 1000 vehicles. The EWD Providers submission to the System Manager would then be assessed to ensure that the infrastructure was commensurate with the number of vehicles being applied for.

* For an example please refer to the IAP Functional & Technical Specification.

As a EWD Providers cliental grows, so does the burden on the EWD Providers System. When the EWD Providers cliental nears the number of vehicles they have been certified for, they must notify the System Manager to demonstrate how they will cater for progressing past their certified numbers of vehicles.

B.10 EWD Provider System*

To maintain continuous operation, the EWD Providers System will need to have business continuity and disaster recover processes commensurate with the number of vehicles being monitored. These processes will need to be documented and kept current within the EWD Providers quality management system.

B.11 Maintenance and continuity of EWD Provider System*

B.12 Documentation of EWD Provider System*

1.2.4 Data handling

As explained previously, communication between the IVU and the EWD Provider should be regular. If this regular communication does not occur, there should be a process in place to be able to recover data from the device.

IVU Data that is received by the EWD Provider should be tested to determine if the IVU may be malfunctioning.

B.13 Data collection*

B.14 Data processing*

B.15 Data testing*

IVU Data that is received by the EWD Provider should be backed up and archived. This ensures that a true and correct copy is recorded which may be required if requested by an authority. In the context of the HVDF Legislation, the EWD Provider may take on some of the responsibilities of the record keeper. This is discussed further under the Fatigue Application chapter.

B.16 Ability to backup and archive data*

1.2.5 Intelligent map

To provide a meaningful location where the work / rest change of the driver occurs in any required reporting (i.e. place names in addition to latitude and longitude), the EWD Provider will be required to retain an electronic map. The map should be approved and issued the System Manager to ensure all participants utilise the same information.

B.17 Intelligent Access Map*

* For an example please refer to the IAP Functional & Technical Specification.

1.2.6 Tier 1 (B2B) and Tier 2 interchange

As regulatory applications will often require some level of communication between a EWD Provider and an Authority, the EWD Provider will require structured and unstructured method of communication.

As a structured communication medium, the EWD Providers will require a B2B interface. As an unstructured communication medium, the EWD Providers will require a secure email facility.

B.18 Tier 1 data interchange – B2B*

B.19 Tier 2 data interchange*

1.2.7 EWD Provider quality system

EWD Providers should have a documented Quality System in place. The Quality System should contain components that control the specification, design, development and ongoing performance of the IVU and EWD Provider System. This Quality System should also control the process of updates and changes and should be in alignment with a recognised Quality Standard.

B.20 EWD Provider Quality System

B.20.5 The specification, design, development and testing of the IVU and EWD Provider System shall employ an established software engineering methodology subject to the approval of the Certifying Authority.

B.20.6 Such a methodology shall be in accordance with HB 171 and specifically address the design elements the developer will employ to maximise the evidentiary value of electronic records.

Note: AS/NZS 12207 sets out a framework for such a methodology however methodologies which do not follow the philosophy contained in AS/NZS 12207 may also be suitable.

The EWD Provider should undergo both internal and external audits to ensure that they continue to provide high quality services. The results of these audits should feed into the Quality System of the EWD Provider for continuous improvement actions. Further, the results should be available for audit by the System Manager.

B.21 Internal and external audits for EWD Provider Quality System*

The EWD Providers should maintain high levels of data security to ensure that their EWD Provider System remains operational. The information security should be in alignment with recognised security management practices.

* For an example please refer to the IAP Functional & Technical Specification.

B.22 Information security

- B.22.6 The EWD Provider shall be required to implement an Information Security Management System (ISMS) necessary for the on-going operation of the system.
- B.22.7 The ISMS shall provide assurance that the risks to evidentially-significant information will be managed appropriately by the users of the system.
- B.22.8 This ISMS shall be in alignment with AS/NZS 27001 and implement control mechanisms in accordance with AS/NZS 27002. The ISMS shall give specific care and focus to:
- driver identification and authentication
 - the management of cryptographic elements of the system including hardware, software and keys
 - physical and environmental security
 - access control, especially access from privileged users and the mechanisms to provide controlled access to functions and information based upon a user's legitimate tasks on a need-to-know basis
 - network and communications security
 - incident detection and management.

To protect the data and information held by the EWD Provider, each provider shall adopt a risk based data access control policy for employees of the provider.

B.23 Data access controls*

To ensure that the Quality System is working, the EWD Provider should have a method to communicate the effectiveness of their Quality System to the System Manager. This should include any future developments or proposed modifications.

B.24 Reporting to System Manager***1.2.8 EWD quality monitoring station**

As the EWD Provider's end to end system will be comprised of a complex arrangement of components (i.e. IVU, telecommunications provider, EWD Provider System etc), it is beneficial for the EWD Provider to maintain a Quality Monitoring Station (QMS). The QMS provides the EWD Provider with a working example of an IVU and enables them to monitor each of the components of their end to end system.

B.25 EWD Provider Quality Monitoring Station***1.2.9 Certification**

To ensure that the EWD Provider's offering meets the Specification requirements within this report, the EWD Provider's offering should be tested. This role, as discussed in Section 4 belongs to a System Manager.

* For an example please refer to the IAP Functional & Technical Specification.

Once certified, an EWD Provider's offering should be audited to ensure that it continues to meet the requirements of the Specification.

B.26 System Manager audit and review*

B.27 IVU audit and review*

B.28 EWD Provider data audit*

B.29 Position audit*

1.2.10 EWD Provider restriction on post-certification change

Given that all components of the system will be approved prior to certification, any updates made to any component of the system after the certification process must be approved by the System Manager. Depending on the scope of the update, this may require the system to be recertified to ensure it continues to meet the specification.

B.30 EWD Provider restriction on post-certification change*

1.3 Specification for Self Declaration Input Device (SDID)

1.3.1 Self Declaration Input Device

To allow a driver to be able to declare when they are working and resting and to possibly manually enter in their personal details and comments, the IVU will need to have a Self Declaration Input Device.

C.1 Self Declaration Input Device (SDID) *

C.2 SDID data entry prompt*

C.3 Non-regulatory applications in SDID*

C.4 SD data*

C.6 SD Comments*

C.7 SDID provision to support IVU type-approval*

* For an example please refer to the IAP Functional & Technical Specification.

2 APPLICATION SPECIFICATION: FATIGUE

2.1 Specification for IVU

2.1.1 *Physical and environmental characteristics*

The HVDF Legislation requires a driver to be able to record their personal details as well as the work and rest performed.

As driving is a subset of the work defined within the HVDF Legislation, the recording of work and rest cannot be simply when the vehicle is on or off. There may be instances where the driver is resting and the vehicle has been turned on or the driver is working when the vehicle is turned off. As such, a driver must be able to declare their work and rest.

The HVDF Legislation requires a driver to be able to annotate why they were not able to make a required rest break and have opportunity to dispute any of the automatically recorded information.

A driver will therefore need an interface for them to toggle between work and rest status and be able to enter in free text.

As discussed within the Section 4, the Austroads Steering Group requires that as a minimum standard, IVUs will be able to be connected to a printer. The printer is required to be able to print the information normally contained on a PWD sheet to allow for unequipped roadside inspectors to view the driver's records. It should be noted that a printer is far from a desirable as it adds cost, complexity, increased maintenance and a significant opportunity for failure. However, as there are a number of unequipped roadside inspectors, until these obtain equipment suitable to review electronic records or roadside inspection is dispensed with, it is a necessary evil.

To enable the portability of driver data between systems, a driver will need to be issued with a driver Recording Device (DRD). This device will need to be interfaced to the IVU.

The European Digital Tachograph uses a smart card as the DRD. This may be the most logical choice for the Australian environment given the introduction of the smartcard based Queensland New driver's Licence. However, until the adoption and commissioning of the smartcard by other Jurisdictions has occurred, mandating the smartcard and its associated infrastructure as the standard DRD may be costly and premature.

AF.1. In-Vehicle Unit

AF.1.1 The IVU shall have a USB interface for a Driver Recording Device (DRD).

The HVDF Legislation requires the IVU must be labelled by with a label supplied by the Authority.

AF.2 EWD labelling

AF.2.1 The IVU shall be labelled with a number provided by the Jurisdiction as a certificate of approval.

The DRD is a USB mass storage device that is issued, controlled and managed by a DRD Issuer. The issuing of a DRD will require a process around identification and authentication of the driver to ensure only one DRD is issued per driver. This may be similar to the mechanism used in the written work diary, i.e. checking the driver against the driver's Licence and recording the details of

the DRD in a national register. The DRD Issuer is also responsible for maintaining the interoperability of DRDs across all IVUs.

The specifications for DRDs are written based on enabling data portability and interoperability while maintaining tamper evidence.

The DRD shall be such that it may be read from and written to, but it shall never have any data deleted. Whilst this may seem like an over complex requirement of the system, it solves the issue of an entity trying to tamper with the device by deleting records and replacing the record.

The DRD has several functions. First, it allows the driver to port data between systems. Thus, it provides a mechanism where 28 days worth of data can follow the driver.

Secondly, the DRD provides a mechanism to provide the last 28 days of data to a new EWD Provider. This case may occur where a driver operates with multiple transport operators running systems installed and maintained by different EWD Providers. As the EWD Providers do not communicate directly with each other, the DRD provides the ability for the new EWD Provider to continue to monitor the compliance of the driver to all potential regulated hours (i.e even compliance based on 14 and 28 days worth of data).

Whilst it is possible to provide authentication and identification of who has authored the records, it is difficult to detect if records have simply been deleted. If the device was only used within one EWD Provider's system, the record numbering would provide evidence of missing records. However, as different EWD Providers will potentially have different record numbering sequences, a EWD Provider cannot use this information to verify if records have been deleted. Thus, by removing the ability for records to be deleted, the EWD Provider can rely on the last 28 days of data on the DRD as the last records recorded for the driver. Then, by verifying that the records have been authored by a certified EWD Provider, the EWD Provider can trust that the records are complete and authentic.

Further, as it is expected that the DRDs will be simply used to hold the driver's declarations, it is expected that this information would be a tiny amount comparative to the industry standard mass storage devices (i.e. memory sticks). For example, it is expected three years worth of SD (Work) and SD (Detail) records would account for less than 100Mb of data.

A driver will be required to obtain a new DRD prior to it being completely filled up. This will require the driver visiting the Authority or an agent of the Authority and being re-identified and authenticated prior to being issued with a new device. The Authority or agent will copy the last 28 days worth of records to the new DRD and fill up the old DRD such that no more records can be stored on the device. Both DRD will then be provided to the driver. This process is similar to obtaining a new written work diary from the Jurisdictions.

AF.3 USB driver Recording Device

AF.3.1 The DRD Issuer shall provide DRDs that store SD (Detail) and SD (Work) Records declared by the drivers.

AF.3.2 A DRD is a Series A plug USB mass storage device.

AF.3.3 A DRD shall be able to:

- a. be written from an IVU
- b. be read by an IVU
- c. prevent any deletion of Records from the DRD.

AF.4 DRD identifier

AF.4.1 Each DRD shall have a unique alphanumeric identifier (DRD ID) that will be used to identify:

- a. the particular DRD
- b. the particular driver.

Note: the DRD Issuer will provide each driver with a unique identifier.

AF.4.2 The DRD ID shall be visibly etched or marked on the outside casing of the unit in a manner such that it cannot be modified or removed.

AF.5 DRD Suitability for use in vehicles

AF.5.1 A DRD shall comply with A.7 when tested as an element of the IVU.

AF.6 DRD documentation

AF.6.1 The EWD Provider shall document how to operate the DRD and supply this documentation to the operator of the vehicle.

AF.6.2 The driver will operate the DRD to the instructions of the manufacturer.

Note: When a driver is first issued with a DRD, the DRD Issuer shall pre-populate at least one SD (Detail) or SD (Work) Record in the DRD before issuing it to the driver. The pre-populated Record shall have the driver's Licence Number, Jurisdiction which issued the driver's licence and the driver's name.

When replacing a DRD for a driver, the DRD Issuer shall copy the Records generated in the last 28 days from the old DRD and paste them onto the new DRD.

2.1.2 Data collection and Record generation

Under the HVDF Legislation, the information a driver must record in their work diary are:

- day of the week
- date
- driver's name
- driver's Licence number
- the name of the jurisdiction where the driver's licence was issued
- whether the driver is operating under standard hours, BFM hours, AFM hours or the hours specified in a work/rest exemption
- the driver's operator's BFM or AFM accreditation number (if the driver is working under BFM or AFM hours or the hours specified in a work/rest hours exemption that was granted in combination with an operator's BFM or AFM accreditation)
- details of the driver's base
- details of the driver's record location
- details of the new base or record location (if the driver changes from one base or record location to another)
- time zone of the driver's base
- nature of each work/rest change
- work or rest time spent since the last work/rest change

- the time and place of the work/rest change
- odometer reading at each work/rest change
- registration number (LPN) of each vehicle the driver drives
- other driver's name, other driver's licence number, other driver's security/identifying work diary number and the name of the jurisdiction that issued that diary (if the driver is or becomes a two-up driver)
- the daily total work time and the daily total rest time (after finishing work for the day).

The information described above may be thought of as:

- a. information that must be recorded once per day
- b. information that must be recorded every work/rest change.

On a WWD, the information recorded at the top of the work diary page must be recorded once per day. The information record in the middle of the page (regarding work and rest changes) must be recorded at each work / rest change.

This concept is extended to the recording of records within the EWD. Two records are required for the recording of the information required by the HVDF Legislation: SD (Detail) and SD (Work).

SD (Details) Records contain the driver identifying information and is consistent with the daily record information in the WWD. SD (Work) Records contain the information pertinent to the work and rest change and is consistent with the information recorded at each work / rest change within the WWD.

SD (Detail) records are required when the driver starts recording information for the day with a particular IVU.

However, a driver may switch between IVUs or EWD Providers. As such, when a driver switches between IVUs, they will need to provide the system with another SD (Detail) Record. This enables the EWD Provider to understand:

- a. if another IVU has been used to record the driver's data; or
- b. what the identifying details are of the driver who has just started using one of the IVUs reporting to it.

AF.7 Self Declaration (SD) Records

AF.7.1 An SD (Detail) Record shall be created at:

- a. the start of each new working day upon declaration of work the first declaration on the IVU for that working day.

Note: as a driver may switch IVUs, it is important to capture the details of the driver at the start of the day and whenever they change IVUs.

AF.7.2 An SD (Work) Record shall be created at each work and rest change.

AF.7.3 An SD (Detail) Record shall consist of at least the following data:

- a. record number
- b. IVU ID
- c. date / time of generation

- d. EWD Functional and Technical Specification Version Number
- e. Driver's Licence number
- f. driver's Licence Issuing Jurisdiction
- g. driver's name
- h. driver's work and rest scheme (STD, BFM, AFM)
- i. address of driver's Base
- j. address of driver's Record Location.

AF.7.4 An SD (Work) Record shall consist of at least the following data:

- a. record number
- b. date / time of generation
- c. EWD Functional & Technical Specification Version Number
- d. driver's Licence number
- e. driver's Licence Issuing Jurisdiction
- f. driver's Name
- g. comment Text
- h. work status (work / rest)
- i. work time or rest time spent since the last work/rest change
- j. odometer reading at the work/rest change
- k. registration number of the heavy vehicle
- l. if driving in a two-up arrangement:
 - other driver's name
 - other driver's licence number
 - other driver's work diary number
 - Jurisdiction that issued other driver's work diary
- m. the last known position of the driver (lat / long);
- n. cumulative daily work time
- o. cumulative daily rest time.

AF.7.5 The last known position of the driver (lat / long) shall be populated from the preceding non-blank / void Position Record.

AF.7.6 At a minimum, the driver's name, driver Licence number, driver's Licence issuing Jurisdiction with SD (Detail) and SD (Work) Records shall be automatically generated when the driver authenticates themselves to the system using the Identification and Authentication method issued by the EWD Provider.

AF.7.7 The driver shall be given an opportunity to confirm the correctness of the record recorded by the IVU.

AF.7.8 If the driver confirms the correctness of the record, the record shall be recorded into the IVU.

AF.7.9 If the driver enters an objection to the record, the record shall be recorded into the IVU with a declaration of the driver's objection contained within the comment text.

To provide identification and to be able to determine completeness, each SD (Detail) and SD (Work) Record will contain a record number. Each record will be assigned a consecutive and increasing number from a sequence large enough such that record shall not contain the same number within a three year period, and shall be different from any other record numbering sequences operating in the IVU.

AF.9 Record Numbering (SD) Records

AF.9.1 SD (Details) and SD (Work) Records shall be assigned record numbers from the one record numbering sequence, with consecutive and increasing record numbers assigned to successive SD Records in order of generation.

AF.9.2 The numbering sequences shall be:

- a. a large enough cycle to ensure that the same Record Numbers shall not be issue more than once every three years
- b. shall be separate to any other IVU Data Record number sequences such that they never clash.

2.1.3 Data Storage and Transfer

SD (Detail) and SD (Work) Records shall be stored on both the IVU and the DRD. The IVU shall store the records until they are transmitted to the EWD Provider. The DRD shall maintain a minimum of 28 days of driver SD (Detail) and SD (Work) Records and store these within a standard format and within a CSV file. The storage onto the DRD in a prescribed format allows the driver to transfer records between systems and continue recording records.

AF.10 DRD Record Storage

AF.10.1 The DRD shall contain either a FAT16 or FAT32 file system.

AF.10.2 The DRD shall contain a top level directory called EWD.

AF.10.3 The IVU shall write DRD records within a CSV file named EWDYYYYMMDDHHMMSS

AF.10.4 The IVU shall store SD Records with the contents specified in Table A – 1 and Table A – 2.

Note: the YYYYMMDDHHMMSS represents the time when the file is created.

AF.11 IVU Data Record storage capability

AF.11.1 The IVU shall be capable of storing at least 2000 SD (Detail) and SD (Work) Records.

Note: SD (Detail) and SD (Work) record storage requirements are based on approximately 14 days of operation and 40 SD (Detail) and 100 SD (Work) Records being produced per day.

AF.12 DRD Data Record storage capability

AF.12.1 The DRD shall be capable of storing a minimum of three years of SD (Detail) and SD (Work) Records in plain text.

Note: Based on the assumption of approximately 40 SD (Detail) and 100 SD (Work) Records per day of operation, it is expected that the required size of the DRD would be less than 100Mb.

AF.12.2 The DRD shall not delete or overwrite any records.

AF.12.2 The IVU shall warn the driver when 95% of the memory in the DRD has been used.

Table A – 1: Data format for SD (Detail) Records

Number	Name	Use	Format	Notes
SDD001	Date	Mandatory	YYYYMMDD	Date in the timezone of Driver's base
SDD002	Time	Mandatory	HHMMSS	Time in the timezone of Driver's base
SDD003	IVU ID	Mandatory	AN (9)	IVU identifier
SDD004	Record Number	Mandatory	N (6)	As recorded by the IVU
SDD005	EWD F&T Spec Version Number	Mandatory	D (4.2)	Version number of the Specification
SDD006	Driver's Licence Number	Mandatory	N (9)	9-digit number
SDD007	Driver's Licence Issuing Jurisdiction	Mandatory	AN (3)	3 letters representing the State/Territory. If the State/Territory has only 2 letters, the last letter shall be populated with a space
SDD008	Driver's name	Mandatory	AN (40)	Driver's name, A space shall be use between two words in the name.
SDD009	Driver's work and rest scheme (STD, BFM, AFM)	Mandatory	AN (3)	3 characters represent work and rest scheme
SDD010	Accreditation number (BFM and AFM only)	Mandatory*	AN (8)	Accreditation number for BFM or AFM
SDD011	Driver's Base Latitude	Mandatory	D (9.5)	Signed decimal degrees (GDA94) from -90.00000 to +90.00000, for example -12.34567
SDD012	Driver's Base Longitude	Mandatory	D (10.5)	Signed decimal degrees (GDA94) from -180.00000 to +180.00000, for example +123.45678
SDD013	Record Position Latitude	Mandatory*	D (9.5)	Signed decimal degrees (GDA94) from -90.00000 to +90.00000, for example -12.34567
SDD014	Record Position Longitude	Mandatory*	D (10.5)	Signed decimal degrees (GDA94) from -180.00000 to +180.00000, for example +123.45678
SDD015	Number of Satellites	Mandatory	N (2)	
SDD016	HDOP	Mandatory	D (4.1)	Decimal value

* shall be filled with spaces if no data is available

Note: The following is an example SD (Detail) Record (spaces have been shown as '^' and artificial filed separators (|) have been inserted purely for clarity in this document):

20091113|123456|ABC000001|123456|01.01|987654321|VIC|SMITH^JONES^|BFM|123/4567|39.12312|+141.12345|39.12456|+141.12789|04|000.1<CR><LF>

Table A – 2: Data format for SD (Work) Records

Number	Name	Use	Format	Notes
SDW001	Date	Mandatory	YYYYMMDD	Date in the timezone of Driver's base
SDW002	Time	Mandatory	HHMMSS	Time in the timezone of Driver's base
SDW003	IVU ID	Mandatory	AN (9)	IVU identifier
SDW004	Record Number	Mandatory	N (6)	As recorded by the IVU
SDW005	EWD F&T Spec Version Number	Mandatory	D (4.2)	Version number of the Specification
SDW006	Driver's Licence Number	Mandatory	N (9)	9-digit number
SDW007	Driver's Licence Issuing Jurisdiction	Mandatory	AN (3)	3 letters representing the State/Territory. If the State/Territory has only 2 letters, the last letter shall be populated with a space
SDW008	Driver's name	Mandatory	AN (40)	Driver's name, A space shall be used between two words in the name.
SDW009	Work/Rest status	Mandatory	N (1)	0 – Rest 1 – Work
SDW010	Work time or Rest time spent since the last Work/Rest change	Mandatory	DDHHMMSS	If Work/Rest status = 0, this represents Work time; if Work/Rest status = 1, this represents Rest time.
SDW011	Odometer reading at the Work/Rest change	Mandatory	D (9.1)	Odometer reading
SDW012	Registration number of the heavy vehicle	Mandatory	AN (7)	Registration number
SDW013	Registration Jurisdiction of the heavy vehicle	Mandatory	AN (3)	3 letters representing the State/Territory. If the State/Territory has only 2 letters, the last letter shall be populated with a space
SDW014	Two-up arrangement status	Mandatory	N (1)	0 – single Driver 1 – two-up Driver
SDW015	The other Driver's name	Mandatory*	AN (40)	The other Driver's name. To be populated with space if only single Driver
SDW016	Other driver's licence number	Mandatory*	N (9)	9-digit number
SDW017	Other driver's work diary number	Mandatory*	AN (7)	DRD ID or work diary number
SDW018	Jurisdiction that issued other driver's work diary	Mandatory*	AN (3)	3 letters representing the State/Territory.
SDW019	The last known position Latitude	Mandatory	D (9.5)	Signed decimal degrees (GDA94) from -90.00000 to +90.00000, for example -12.34567
SDW020	The last known position Longitude	Mandatory	D (10.5)	Signed decimal degrees (GDA94) from -180.00000 to +180.00000, for example +123.45678
SDW021	Cumulative daily Work time	Mandatory	HHMMSS	Sum of all Work times for the day
SDW022	Cumulative daily Rest time	Mandatory	HHMMSS	Sum of all Rest times for the day
SDW023	Comment text	Mandatory*	AN (40)	Comment from the Driver

* shall be filled with spaces if no data is available

Note: The following is an example SD (Work) Record (spaces have been shown as '^' and artificial field separators (|) have been inserted purely for clarity in this document):

```
20091113|123456|ABC000001|123456|01.01|987654321|VIC|SMITH^JONES^|1|000010134|0087654.3|^ABC123|VIC|0|^
^|39.12312|^+141.12345|020348|000000|^<CR><LF>
```

The data stored within the DRD must be evident of change and must clearly show who has authored the record. Whilst the licence number within the record shows who has declared the record, it is important to identify that this was created through an approved certified system.

One of the simplest ways to achieve this evidence is to digitally sign the records with a signature created using certificates with a known integrity. The use of such digital signatures and certificates allows for users to verify that the records are complete, has not been changed and provides a non-repudiation of the author of the records.

Simplistically, the EWD Provider shall apply for the ABN-DSC certificate. Each IVU shall contain the private certificate of the EWD Provider. Each Data Block created on the DRD will be digitally signed using the private certificate. Accompanying the signature, each Data Block shall contain the public certificate which may be used to verify the data and the author of the data.

AF.13 DRD Data security

AF.13.1 Each EWD data file shall have an accompanying EWD signature file.

AF.13.2 The name of the EWD signature file shall be derived from the name of the EWD data file by replacing the ".csv" file extension with a ".p7s.b64" file extension.

Note: For example, an EWD data file "abcd.csv" shall have an EWD signature file named "abcd.p7s.b64".

AF.13.3 The EWD signature file shall contain a BASE64 encoded cryptographic Message Syntax (CMS) digital signature for the entire EWD data file:

- a. The digital signature shall not include the signed data
- b. The digital signature shall be formed using the SHA-1 message digest algorithm
- c. The digital signature shall include the full certificate chain for the signer's PKI certificate.

AF.13.4 The EWD Provider shall be responsible for the management of the private key.

AF.13.5 The EWD Provider shall document the key management process to the satisfaction of the System Manager.

2.1.4 Authentication

Each driver when making declarations within to the IVU shall need to identify and authenticate themselves to the system. This ensures that records generated by the self declaration have been based upon the action of the driver rather than an imposter.

The authentication of the identity of the user of a EWD can be implemented using a number of technologies or approaches. Under a performance based regime, this specification proposes a standard which the authentication mechanism must meet rather than providing the technical specification.

This approach allows for individual EWD Providers to come up with their own techniques to authenticate whilst maintaining an equivalent level of quality between the techniques.

In considering the available guidelines and standards applicable to user authentication in Australia, the most applicable standards are the Commonwealth Government's National e-Authentication Framework (NeAF) (Department of Finance and Deregulation 2009) and the Queensland Government Authentication Framework (QGAF-AC) (Queensland Government 2006). These frameworks have been designed to establish a common set of principles for electronic authentication for interactions with government entities in Australia and represent best practice and are directly applicable to the requirements for authentication in EWD systems.

NeAF defines electronic authentication as:

Electronic authentication (or “e-Authentication”) is the process of determining the degree of confidence that can be placed in assertions that a user or identity is who and/or what they purport to be. Assertions include identity, role, delegation and value. The National e-Authentication Framework (NeAF) is primarily concerned with the electronic authentication of identity. Electronic transactions are considered to be across a number of channels.

e-Authentication is accomplished using something the user knows (e.g. password, secret questions and answers), something the user has (e.g. security token) or something the user is (e.g. biometric), or a combination of these.

QGAF-AC Section 2 expands on the concept of authentication from NeAF as follows:

Authentication is a process that tests a claimant's assertion of their identity against an earlier registration process. Various means are used to support this assertion, known as authentication mechanisms. Examples of commonly used mechanisms are passwords, PIN numbers, One time passwords generated by a device, Software tokens (a key or digital certificate that is stored on removable media), photo identification documents, and hardware devices.

Authentication credentials are supplied to the client after successful registration of the client's identity, and are “objects” that bind an identity to a set of attributes contained in a specific record of registration.

A credential may be as simple as the user's knowledge as in shared information or passwords (a logical object). A credential can also be a “software” device, such as a digital certificate, or a physical object, such as a one-time-password generating device, a magnetic-stripe card, a smart card containing a digital certificate, or a code book. Physical device credentials are also commonly called tokens (though this most correctly refers to the information stored in the device).

Credentials provide a level of confidence that the client returning to the service is in fact the same client that was previously registered. The stronger a credential, the higher the level of confidence a EWD Provider can have that the client returning to the service is in fact the same client that was previously registered.

Both the QGAF-AC and the NeAF-MS define a series of assurance levels to describe the importance of the authentication process and the resultant level of robustness required of an identity authentication solution. The assurance levels are based on the assessment of the risks should the authentication solution fail. The authentication levels are presented in Table A – 3.

Table A – 3: NeAF assurance levels

Assurance Level	Assurance Provided	Description
Level-4	High Assurance	High confidence is required in the identity assertion
Level-3	Moderate Assurance	Moderate confidence is required in the identity assertion
Level-2	Low Assurance	Low confidence is required in the identity assertion
Level-1	Minimal Assurance	Minimal confidence is required in the identity assertion
Level-0	No Assurance	No confidence is required in the identity assertion

QGAf-AC Section 2.2 also provides a summary of the main types of authentication mechanisms commonly found in use, their supported assurance levels and the interaction channels over which they can be used as reproduced in Table A – 4.

Table A – 4: Authentication mechanisms mapped to Assurance levels

	Assurance Levels Possible	Remote Data Channels			Remote Voice Channels		Physical Channels	
		Web	Public Kiosk	Mobile Data Link	Auto Voice Response	Phone + Operator	Mail	Service Counter
PIN	1	Yes	Yes	Yes	Yes	No	No	Yes ⁺⁺
Signature	1,2	No	No	No	No	No	Yes	Yes
Software Token / Certificate	1,2	Yes	No	No	No	No	No	No
Password	1,2	Yes	Yes	Yes	No	No	No	No
Knowledge Based	1,2	Yes	Yes	Yes	Yes	Yes	No	Yes
One Time Password – No PIN or Password	1,2	Yes	Yes	Yes	Yes	Yes	No	Yes
Hardware cryptographic token	1,2	Yes ⁺⁺	Yes ⁺⁺	Yes ⁺⁺	No	No	No	Yes ⁺⁺
Photo Identification Document	1,2,3	No	No	No	No	No	No	Yes
Software Token with PIN or password	1,2,3	Yes	No	No	No	No	No	No
PIN and Card	1,2,3	Yes	Yes	Yes	No	No	No	Yes
Hardware cryptographic token with PIN/Password or Biometric	1,2,3,4	Yes ⁺⁺	Yes ⁺⁺	Yes ⁺⁺	No	No	No	Yes ⁺⁺
One Time Password – Generated or Received with PIN/Password or Biometric	1,2,3,4	Yes	Yes	Yes	Yes	Yes	No	Yes

NeAF and QGAF-AC both recognise that the specific authentication mechanism appropriate for a system will in part be determined by the specific capabilities of the system, supplier preferences and/or operator-specific preferences. Of particular importance is the recognition that there will be different solutions each of which provides the same level of assurance and it is not appropriate to constrain a system provider in choice of solution so long as the risk is appropriately managed.

The NeAF document set, established to address identity authentication issues, recommends an approach based on the development of a risk management strategy for the identity authentication requirements and the assessment of specific identity authentication processes against the strategy in order to have assurance that the system provides appropriate management of the risks.

A framework for the development of a risk management strategy for a system and the risk assessment for proposed solutions are contained in the NeAF-Vol1 document *“Better Practice Guidelines – Identity e-Authentication”*.

AF.14 Authentication

AF.14.1 The IVU shall incorporate, subject to the approval of the System Manager, a method of driver identification and authentication based upon the NeAF methodology.

AF.14.2 The identification and authentication methodology shall provide at least a NeAF assurance level 3.

2.1.5 Outputs

The HVDF Legislation requires that for an Electronic Work Diary to be approved, it must be able to indicate to the driver that the system is, or is not, working properly.

AF.15 Functionality indicator

AF.15.1 The IVU shall contain a visual indication that the IVU is functioning properly.

AF.15.2 The IVU shall contain a visual indication that the IVU is not functioning properly.

2.2 Specification for EWD Provider

2.2.1 Data handling

A critical function described under the HVDF Legislation is the archival of driver declaration records. This responsibility is bestowed upon the record keeper. The HVDF Legislation defines the record keeper as one of three entities: employed driver, self-employed driver or an operator. However, the HVDF Legislation also allows the record keeper to engage the services of another person to carry out some or all of their functions.

Whilst not mandated, in an electronic environment it would be logical to engage a EWD Provider to perform the data storage task for the record keeper. Under this obligation, the EWD Provider shall abide by the legislative archival arrangements.

If the EWD Provider is not acting as the record keeper, it is still important to maintain a record of the driver's declarations in case a question is raised on the collection process. As such, in this scenario records shall be stored for a minimum of one year. However, if the EWD Provider is acting as the record keeper, the records shall be stored for a minimum of three years.

BF.1 Data backup and archiving

BF.1.1 If the EWD Provider is performing the data storage task for the record keeper, the EWD Provider shall:

- maintain all records for a minimum of 3 years
- protected records from deletion or modification for three years
- must keep the records at the record location so that they are reasonably accessible to an authorised officer or police officer
- provide access to the record keeper to read the records that they are required to keep
- provide a print out to the record keeper of their drivers' records for any relevant day on which the driver was using an EWD.

BF.1.2 If the EWD Provider is not performing the data storage task for the record keeper, the EWD Provider shall maintain all records for a minimum of one year after successful transmission to the record keeper.

2.2.2 Identification of Non-compliance and issuing of NCRs

One of the greatest advantages to converting the paper based records to electronic records is the ability to perform computation on the records. A very simple task would be to use the electronic records to calculate whether the driver's working time is compliant with the regulated working time. Whilst the HVDF Legislation is silent on the reporting of non-compliance, it is foreseeable that the future may require the EWD Provider to be able to produce a report on the non-compliance and route that report to the Authority, the Transport Operator or any of the other entities named within the HVDF Legislation.

Further, it is expected that as tampering with an electronic work diary is an offence under the HVDF Legislation, a EWD Provider will be requested by the Authority to report this information.

As drivers may operate between multiple systems, the DRD will be required to be read from as well as written to. The DRD will provide the new system with the last 28 days worth of driver work and rest data.

As the DRD will allow open access to reading and writing (but not deleting) it will be a requirement of the EWD Provider to verify that the data on the device has been written to by a legitimate source (i.e. another certified EWD Providers IVU). If the device has been written to by an illegitimate source, then the EWD Provider will be required to notify the Authority.

A list of the certified EWD Providers will be issued to EWD Providers by the System Manager.

Whilst an Authority is expected to maintain a B2B interface, it is expected the other entities named within the HVDF will not. As such, these reports may be sent via a secure email facility and may be rendered into a plain text version.

<u>BF.2 Non-Compliance Reports (NCRs)*</u> <u>BF.3 NCR Position Records and NCR Speed Records*</u> <u>BF.4 Alarm NCRs*</u>
<u>BF.5. Illegitimate Author of Records</u> BF.5.1. The IVU shall be required to check that Records on the DRD connected that have been generated within the last 28 days have been authored by a Certified EWD Provider. BF.5.2 If the EWD Provider detects that Records generated within the last 28 days have been authored by an entity other than a certified EWD Provider, the EWD Provider shall issue an Alarm NCR. <i>Note: a list of certified EWD Providers will be provided to each certified EWD Provider by the System Manager.</i>
<u>BF.6 Configurable NCR routing</u> BF.6.1 The NCRs provided to the Authority or parties other than the Authority shall be configurable such that their generation may be suppressed upon instruction by the Authority.
<u>BF.7 Assessment of SD (Detail) and SD (Work) against Conditions</u> BF.7.1 When assessing SD (Work) non-compliance, the applicable conditions shall be those provided by the Authority(s) and shall pertain to the date/time and vehicle position as specified in the Position Record and shall use the driver's declaration of work and rest as specified within the SD (Work) Record. BF.7.2 For each Position Record the EWD Provider shall assess the SD (Work) non-compliance using: - the most recent SD (Work) Record, irrespective of the Jurisdiction in which it was generated; and - the applicable conditions identified for that Position Record. <i>Note: the business rules regarding the generation of the SD (Work) NCR have yet to be determined and shall be based upon policy.</i>
<u>BF.8 NCRs to non-Authorities</u> BF.8.1 The EWD Provider shall be able to provide NCRs, in plain text, to parties other than the Authority upon request by the Authority. BF.8.2 These NCRs shall be provided by secure email as prescribe within Tier 2 communications. BF.8.3 The secure email shall incorporate a notification of successful transmission of the NCR to the intended recipient. <i>Note: see also B.19</i>

2.2.3 EWD Registration Process

For an EWD system to provide equivalence with the WWD a comparable method of registering the driver for use with the EWD system is necessary. The current method used by the Jurisdictions for the PWD incorporates:

- Positive identification of the driver by an independent, authorised officer with capture of the driver's details authenticated by the driver's driving licence.

* For an example please refer to the IAP Functional & Technical Specification.

- Creation of a baseline authenticator for the driver by the witnessed entry of the driver's signature in the front of the WWD. This baseline authenticator is then available for comparison to the authenticator (i.e. driver's signature) on subsequent daily sheets in the PWD.
- Controlled allocation of a physical WWD to the diary, which is uniquely identified by a PWD Security Number.
- Recording of the details of the issuance of the diary including who issued the diary, where and when.
- Maintenance of a register of WWDs on issue and the driver to whom they have been issued. This register is available for interrogation by an Authorised Officer.

The process for authorising a driver to use a specific EWD System needs to incorporate equivalent levels of integrity and record keeping to the WWD. Records of the process must be retained by the issuer such that these records can be subjected to later investigation and audit. Upon completion of the process the driver would be issued with appropriate credentials for accessing the EWD system and these credentials can with confidence be relied upon such that when the EWD system is presented with them the system can authenticate the person using those credentials as being the person to whom that credentials were allocated.

BF.9 Driver Registration Process

- BF.9.1 Prior to issuing a driver with their Identification and Authentication method, the EWD Provider shall verify the identity of the driver against their current driver's licence.
- BF.9.2 The EWD Provider shall issue the driver Identification and Authentication method with the details authenticated by the driver's driving licence.
- BF.9.3 The EWD Provider shall maintain a register of all drivers authorised to use the Identification and Authentication method.
- BF.9.4 The EWD Provider shall maintain records concerning the authorisation process including who the officer performing the authorisation was.
- BF.9.5 The EWD Provider shall implement a de-authorisation process through which a driver's authority to access the system will be revoked.
- BF.9.6 Upon de-authorisation, the EWD Provider shall remove the ability of the authentication credentials allocated to the driver to enable access to the EWD System.
- BF.9.7 The EWD Provider shall maintain a register of all drivers that are no longer authorised to use the identification and authentication method for a period of one year after the cancellation of authorisation of this method.

2.2.4 Provision of Records to the record keeper

Under the HVDF Legislation, the record keeper may engage others to perform some of their tasks such as the archival of driving records. However, if the record keeper retains these obligations, the EWD Provider shall provide the records of the driver within 21 days of their generation.

BF.10 Provision of Records to the record keeper

- BF.10.1 If the EWD Provider is not providing the data storage task for the record keeper, the EWD Provider shall provide a driver's SD (Detail) and SD (Work) Records within 21 days of their declaration.

3 APPLICATION SPECIFICATION: SPEED

3.1 Specification for IVU

The decision reached on the 7th November 2008 at the ATC required a specification for both a fatigue and speed monitoring system (ATC 2008). Whilst a significant amount of work has been conducted in the area of what defines a speed offence, the work has been based around the context of a speed non-compliance being detected at point in time rather than from a continuous monitoring device.

For example, traditional methods of speed non-compliance and offence penalties are based around the probability of being caught and the size of the non-compliance. As the probability of being caught with traditional methods is relatively low, the penalties are high. With a continuous monitoring device, every breach of the speed limit is able to be determined. This may result in hundreds or thousands of speeding breaches in a typical trip between Melbourne and Sydney.

As such, considerable work is required in defining what shall be considered a breach of the speed zone and when an offence should be triggered.

Critical to the ability of accurately assessing the speed of a vehicle against the speed zone the vehicle is within, is the availability of a national speed dataset upon which the current vehicle speed can be compared and assessed for compliance. At the time of writing, no such government endorsed dataset exists. However, many Jurisdictions are building a dataset which would ultimately be concatenated to form a nation dataset.

Prior to all of this work being completed, the specification for a speed monitoring system cannot be completed. As such, the specification around speed concentrates on the collection and recording of speed data and provisions for the speed to be assessed against speed zones.

3.1.1 Data collection and record generation

Until the speed compliance strategy is determined, all speed records will need to be captured and stored. It may be possible to reduce this storage requirement if policy dictates that compliant records are not required to be kept, such as in IAP.

Further, it is expected that as speed monitoring will be a contentious issue, there will be a significant amount of policy work prior to a driver being monitored for speed. As such, the monitoring of speed shall be configurable (i.e. on or off) by the EWD Provider.

It is expected that the recording of speed records shall require the inclusion of the driver's details.

AS.1 Speed Records

AS.1.1 The collection and storage of Speed Records shall be configurable (on/off) by the EWD Provider and based upon instruction of the Authority.

AS.1.2 Speed Records shall contain the additional fields of:

- a. driver's Licence number
- b. driver's Licence Issuing Jurisdiction
- c. driver's name.

AS.1.3 The population of these fields shall be based upon the information acquired from the identification and authentication method provided by the EWD Provider.

3.1.2 Storage, display and transfer

The IVU shall store records prior to them being transferred to the EWD Provider. The size of the record storage shall be such that the IVU shall be able to collect records for a period of two weeks and 24 hour operation without communicating to the EWD Provider.

AS.2 IVU Data Record Storage Capability

AS.2.1 The IVU shall be capable of storing at least 400,000 Speed Records.

Note: These storage requirements are based on approximately 14 days of 24 hour operation.

3.1.3 Authentication

As discussed within the Fatigue Application Section, a driver shall need to be identified and authenticate this identification to the system when working. This functionality shall also be required under speed monitoring where the driver identification is necessary.

As such, the IVU shall be able to capture the driver's identity and authenticate that the driver is actually driving.

AS.3 Authentication

AS.3.1 The IVU shall incorporate, subject to the approval of the System Manager, a method of driver Identification and Authentication based upon the NeAF methodology.

AS.3.1 The Identification and Authentication methodology shall provide at least a NeAF assurance level 3.

3.2 Specification for EWD Provider

3.2.1 Identification of Non-compliance and issuing of NCRs

Once the records from the IVU have been received by the EWD Provider, it is then possible to assess these records against the relevant speed zone to determine if the driver is non-compliant.

It is not possible to provide a specification for the issue of the non-compliance until the policy on what triggers and constitutes a NCR is determined.

However, it is foreseeable that the future may require the EWD Provider to be able to produce a report on the non-compliance and route that report to the Authority, the Transport Operator or any of the other entities named within the relevant speed legislation.

BS.1 Non-Compliance Reports (NCRs)*

BS.2 NCR Position Records and NCR Speed Records*

BS.3. Configurable NCR routing

BS.3.1. The NCRs provided to the Authority or parties other than the Authority shall be configurable such that their generation may be suppressed upon instruction by the Authority.

* For an example please refer to the IAP Functional & Technical Specification.

BS.4 Speed Compliance

Note: the business rules regarding the generation of the Speed NCRs have yet to be determined and shall be based upon policy.

BS.5 Speed NCR

BS.5.1 The EWD Provider shall have the ability to produce a Speed NCR.

Note: the business rules regarding the generation of the Speed NCRs have yet to be determined and shall be based upon policy.

BS.6. NCRs to non-Authorities

BS.6.1 The EWD Provider shall be able to provide NCRs, in plain text, to parties other than the Authority upon request by the Authority.

BS.6.2 These NCRs shall be provided by secure email as prescribe within Tier 2 communications.

BS.6.3 The secure email shall incorporate a notification of successful transmission of the NCR to the intended recipient.

Note: see also B.19

APPENDIX B – NTC POSITION ON THE EWD

This is the NTC's position on the requirements of an EWD. Compared to the Specified EWD, this specification has a few major differences:

1. GPS is not required, therefore no automatic work/rest record or position record is captured.
2. The IVU is not required to be tethered to the vehicle.
3. No tamper monitoring is required for the system.
4. A printer is required to provide print out of records at roadside.

This specification contains three parts: In-Vehicle Unit (IVU), EWD Provider System, and Self Declaration Input Device (SDID).

The numbering in this Appendix follows the numbering in the Specified EWD for easy reference.

Part A – Specification for In-Vehicle Unit (IVU)

Physical and environmental characteristics

A.3 Documentation (for IVU)

- A.3.1 The EWD Provider shall document, to the satisfaction of the System Manager, the IVU and all components, cabling and their interfaces.

A.4 IVU identifier

- A.4.1 Each IVU shall have a unique alphanumeric identifier (IVU ID) that will be used to identify:
- a. the particular IVU
 - b. data from that IVU, when being processed or stored by the EWD Provider System.

Note: The System Manager will provide each EWD Provider with a unique, three character identifier which the EWD Provider shall use as a prefix in the IVU identifier (IVU ID).

- A.4.2 The IVU ID shall be visibly marked on the outside casing of the unit as well be stored in the non-volatile programmable read-only memory of the IVU.

A.5 Security seal

- A.5.1 The IVU shall be protected to ensure detection of any unauthorised removal or opening of the IVU.

A.6 Self Declaration capability

- A.6.1 The IVU shall be capable of accepting input from a Self Declaration Input Device (SDID) installed by the EWD Provider.

A.7 Suitability for use in vehicles

- A.7.1 The EWD Provider shall provide to the System Manager, evidence of compliance from an appropriate body to demonstrate the suitability for use in vehicles for the IVU and all associated components.

A.8 Non-regulatory functionality in the IVU

- A.8.1 It shall be permissible, subject to the approval of System Manager for non-regulatory functionality to be accommodated within the IVU.
- A.8.2 The regulatory functionality shall be isolated from any non-regulatory functionality that may be provided by the IVU.
- A.8.3 The EWD Provider shall document, to the satisfaction of the System Manager, any non-regulatory functionality to be provided by the IVU.

Data collection and record generation

A.16 Vehicle odometer data

A.16.1 The IVU shall be able to record the odometer reading at every work/rest change.

A.16.2 The odometer reading shall be stored to a resolution of 1 km.

Note: the odometer reading may be an automatically or manually acquired.

A.22 Record numbering

A.22.1 Location, Alarm and SD Records shall be assigned record numbers from the one record numbering sequence, with consecutive and increasing record numbers assigned to successive IVU Data Records in order of generation.

A.22.2 Speed Records shall be assigned record numbers from a separate numbering sequence, with consecutive and increasing record numbers assigned to successive Speed Records in order of generation.

Storage, display and transfer

A.23 IVU Data Record storage capability

A.23.1 The IVU shall be capable of storing at least 20,000 Location, Alarm and SD Records (combined) and at least 200,000 Speed Records.

Note: This approach is for evidentiary reasons. It prohibits the overwriting of data already collected, albeit at the expense of collecting new data.

A.24 IVU external power supply failure/shutdown

A.24.1 A.24.1 In the event that the external power supply supporting the IVU fails or shuts down, the IVU shall be capable of retaining stored data and monitoring the status of the movement sensors for a period defined by the System Manager.

A.25 Data security and confidentiality measures

A.25.1 It shall not be possible for collected or stored data or software memory within the IVU to be accessible or capable of being manipulated by any person, device or system (including the SDID), other than that authorised by the EWD Provider.

A.26 IVU communication capability

A.26.1 The IVU shall be capable of communicating with the EWD Provider from at least the areas nominated by the EWD Provider.

A.26.2 The channel for the transmission of IVU Data Records to the EWD Provider shall be secure and guarantee standards for privacy and data integrity to the level defined by the System Manager.

Note: For instance, selected communications networks and coverage could be:

a. some form of commercial mobile phone service area; or

b. Australia-wide service area by alternative means.

A.27 Transfer of data from IVU to EWD Provider

A.27.1 The transfer of stored data from the IVU to the EWD Provider shall be performed at least once every 24 hours provided that the IVU is in the communication coverage area offered by the EWD Provider and the vehicle is in operation.

A.27.2 IVU Data Records stored in the IVU shall only be deleted after such data is transferred from the IVU and successful receipt is confirmed by the EWD Provider.

Note: Communications protocols and associated handshaking for data transfers are defined by the EWD Provider.

A.28 IVU Data Records

- A.28.1 IVU Data Records shall be transferred from the IVU to the EWD Provider.
- A.28.2 Every transfer shall include framing data that identifies its sequential order, IVU ID, version number of IVU component plus software and ability to decode or decompress data.

A.29 Integrity and origin of Data Blocks and IVU Data Records

- A.29.1 The numbering shall be sequential.
- A.29.2 Each transfer shall contain error detection and error correction coding that operates successfully.
- A.29.3 Each transfer shall support a form of data authentication (i.e. some form of message authentication only known and accessible to the EWD Provider), subject to the approval of the System Manager, that can prove the origin and integrity of the IVU Data Records.
- A.29.4 The EWD Provider shall document, to the satisfaction of the System Manager, the transfer authentication mechanism.

A.30 Integrity and origin of SD Data

- A.30.1 Similar to the integrity of the communication channel between the IVU and the EWD Provider, the SDID should ensure that there is integrity, confidentiality and authenticity of the driver declaration data.

A.31 IVU approval

- A.31.1 To facilitate IVU approval testing, multiple IVUs shall be provided to the System Manager.

AF.1. In-Vehicle Unit

- AF.1.1 The IVU shall have a USB interface for a Driver Recording Device (DRD).

AF.2 EWD labelling

- AF.1.2 The IVU shall be labelled with a number provided by the Jurisdiction as a certificate of approval.

AF.3 USB Driver Recording Device

- AF.3.1 The DRD Issuer shall provide DRDs that store SD (Detail) and SD (Work) Records declared by the driver.
- AF.3.2 A DRD is a Series A plug USB mass storage device.
- AF.3.3 A DRD shall be able to:
- be written from an IVU
 - be read by an IVU
 - prevent any deletion of Records from the DRD.

AF.4 DRD identifier

- AF.4.1 Each DRD shall have a unique alphanumeric identifier (DRD ID) that will be used to identify:
- the particular DRD
 - the particular Driver.
- Note: the DRD Issuer will provide each Driver with a unique identifier.*
- AF.4.2 The DRD ID shall be visibly etched or marked on the outside casing of the unit in a manner such that it cannot be modified or removed.

AF.5 DRD Suitability for use in vehicles

- AF.5.1 A DRD shall comply with A.7 when tested as an element of the IVU.

AF.6 DRD documentation

AF.6.1 The EWD Provider shall document how to operate the DRD and supply this documentation to the operator of the vehicle.

AF.6.2 The driver will operate the DRD to the instructions of the manufacturer.

Note: When a driver is first issued with a DRD, the DRD Issuer shall pre-populate at least one SD (Detail) or SD (Work) Record in the DRD before issuing it to the driver. The pre-populated Record shall have the Driver's Licence Number, Jurisdiction which issued the driver's licence and the driver's name.

When replacing a DRD for a Driver, the DRD Issuer shall copy the Records generated in the last 28 days from the old DRD and paste them onto the new DRD.

Data collection and Record generation

AF.7 Self Declaration (SD) Records

AF.7.1 An SD (Detail) Record shall be created at:

- a. the start of each new working day upon declaration of work
- b. the first declaration on the IVU for that working day.

Note: as a driver may switch IVUs, it is important to capture the details of the driver at the start at the start of the day and whenever they change IVUs.

AF.7.2 An SD (Work) Record shall be created at each work and rest change.

AF.7.3 An SD (Detail) Record shall consist of at least the following data:

- a. record number
- b. IVU ID
- c. date / time of generation
- d. EWD Functional and Technical Specification Version Number
- e. driver's Licence number
- f. driver's Licence Issuing Jurisdiction
- g. driver's name
- h. driver's work and rest scheme (STD, BFM, AFM)
- i. address of Driver's Base
- j. address of Driver's Record Location.

AF.7.4 An SD (Work) Record shall consist of at least the following data:

- a. record number
- b. date / time of generation
- c. EWD Functional & Technical Specification Version Number
- d. driver's Licence number
- e. driver's Licence Issuing Jurisdiction
- f. driver's Name
- g. comment Text
- h. work status (work / rest)

- i. work time or rest time spent since the last work/rest change
- j. odometer reading at the work/rest change
- k. registration number of the heavy vehicle
- l. if driving in a two-up arrangement:
 - other driver's name
 - other driver's licence number
 - other driver's work diary number
 - Jurisdiction that issued other driver's work diary
- m. the last known position of the driver (lat / long);
- n. cumulative daily work time
- o. cumulative daily rest time.

AF.7.6 At a minimum, the driver's name, driver's Licence number, driver's Licence issuing Jurisdiction with SD (Detail) and SD (Work) Records shall be automatically generated when the driver authenticates themselves to the system using the Identification and Authentication method issued by the EWD Provider.

AF.7.7 The driver shall be given an opportunity to confirm the correctness of the record recorded by the IVU.

AF.7.8 If the driver confirms the correctness of the record, the record shall be recorded into the IVU.

AF.7.9 If the driver enters an objection to the record, the record shall be recorded into the IVU with a declaration of the driver's objection contained within the comment text.

AF.9 Record Numbering (SD) Records

AF.9.1 SD (Details) and SD (Work) Records shall be assigned record numbers from the one record numbering sequence, with consecutive and increasing record numbers assigned to successive SD Records in order of generation.

AF.9.2 The numbering sequences shall be:

- a. a large enough cycle to ensure that the same Record Numbers shall not be issue more than once every three years
- b. shall be separate to any other IVU Data Record number sequences such that they never clash.

Data Storage and Transfer

AF.10 DRD Record Storage

AF.10.1 The DRD shall contain either a FAT16 or FAT32 file system.

AF.10.2 The DRD shall contain a top level directory called EWD.

AF.10.3 The IVU shall write DRD records within a CSV file named EWDYYYYMMDDHHMMSS

AF.10.4 The IVU shall store SD Records with the contents specified in Table A – 1 and Table A – 2.

Note: the YYYYMMDDHHMMSS represents the time when the file is created.

Table A – 1: Data format for SD (Detail) Records

Number	Name	Use	Format	Notes
SDD001	Date	Mandatory	YYYYMMDD	Date in the timezone of Driver's base
SDD002	Time	Mandatory	HHMMSS	Time in the timezone of Driver's base
SDD003	IVU ID	Mandatory	AN (9)	IVU identifier
SDD004	Record Number	Mandatory	N (6)	As recorded by the IVU
SDD005	EWD F&T Spec Version Number	Mandatory	D (4.2)	Version number of the Specification
SDD006	Driver's Licence Number	Mandatory	N (9)	9-digit number
SDD007	Driver's Licence Issuing Jurisdiction	Mandatory	AN (3)	3 letters representing the State/Territory. If the State/Territory has only 2 letters, the last letter shall be populated with a space
SDD008	Driver's name	Mandatory	AN (40)	Driver's name, A space shall be use between two words in the name.
SDD009	Driver's work and rest scheme (STD, BFM, AFM)	Mandatory	AN (3)	3 characters represent work and rest scheme
SDD010	Accreditation number (BFM and AFM only)	Mandatory*	AN (8)	Accreditation number for BFM or AFM
SDD011	Driver's Base Latitude	Mandatory	D (9.5)	Signed decimal degrees (GDA94) from -90.00000 to +90.00000, for example -12.34567
SDD012	Driver's Base Longitude	Mandatory	D (10.5)	Signed decimal degrees (GDA94) from -180.00000 to +180.00000, for example +123.45678
SDD013	Record Position Latitude	Mandatory*	D (9.5)	Signed decimal degrees (GDA94) from -90.00000 to +90.00000, for example -12.34567
SDD014	Record Position Longitude	Mandatory*	D (10.5)	Signed decimal degrees (GDA94) from -180.00000 to +180.00000, for example +123.45678
SDD015	Number of Satellites	Mandatory	N (2)	
SDD016	HDOP	Mandatory	D (4.1)	Decimal value

* shall be filled with spaces if no data is available

Note: The following is an example SD (Detail) Record (spaces have been shown as '^' and artificial filed separators (|) have been inserted purely for clarity in this document):

20091113|123456|ABC000001|123456|01.01|987654321|VIC|SMITH^JONES^|BFM|123/4567|39.12312|+141.12345|39.12456|+141.12789|04|000.1<CR><LF>

Table A – 2: Data format for SD (Work) Records

Number	Name	Use	Format	Notes
SDW001	Date	Mandatory	YYYYMMDD	Date in the timezone of Driver's base
SDW002	Time	Mandatory	HHMMSS	Time in the timezone of Driver's base
SDW003	IVU ID	Mandatory	AN (9)	IVU identifier
SDW004	Record Number	Mandatory	N (6)	As recorded by the IVU
SDW005	EWD F&T Spec Version Number	Mandatory	D (4.2)	Version number of the Specification
SDW006	Driver's Licence Number	Mandatory	N (9)	9-digit number
SDW007	Driver's Licence Issuing Jurisdiction	Mandatory	AN (3)	3 letters representing the State/Territory. If the State/Territory has only 2 letters, the last letter shall be populated with a space
SDW008	Driver's name	Mandatory	AN (40)	Driver's name, A space shall be used between two words in the name.
SDW009	Work/Rest status	Mandatory	N (1)	0 – Rest 1 – Work
SDW010	Work time or Rest time spent since the last Work/Rest change	Mandatory	DDHHMMSS	If Work/Rest status = 0, this represents Work time; if Work/Rest status = 1, this represents Rest time.
SDW011	Odometer reading at the Work/Rest change	Mandatory	D (9.1)	Odometer reading
SDW012	Registration number of the heavy vehicle	Mandatory	AN (7)	Registration number
SDW013	Registration Jurisdiction of the heavy vehicle	Mandatory	AN (3)	3 letters representing the State/Territory. If the State/Territory has only 2 letters, the last letter shall be populated with a space
SDW014	Two-up arrangement status	Mandatory	N (1)	0 – single Driver 1 – two-up Driver
SDW015	The other Driver's name	Mandatory*	AN (40)	The other Driver's name. To be populated with space if only single Driver
SDW016	Other driver's licence number	Mandatory*	N (9)	9-digit number
SDW017	Other driver's work diary number	Mandatory*	AN (7)	DRD ID or work diary number
SDW018	Jurisdiction that issued other driver's work diary	Mandatory*	AN (3)	3 letters representing the State/Territory.
SDW019	The last known position Latitude	Mandatory	D (9.5)	Signed decimal degrees (GDA94) from -90.00000 to +90.00000, for example -12.34567
SDW020	The last known position Longitude	Mandatory	D (10.5)	Signed decimal degrees (GDA94) from -180.00000 to +180.00000, for example +123.45678
SDW021	Cumulative daily Work time	Mandatory	HHMMSS	Sum of all Work times for the day
SDW022	Cumulative daily Rest time	Mandatory	HHMMSS	Sum of all Rest times for the day
SDW023	Comment text	Mandatory*	AN (40)	Comment from the Driver

* shall be filled with spaces if no data is available

Note: The following is an example SD (Work) Record (spaces have been shown as '^' and artificial field separators (|) have been inserted purely for clarity in this document):

20091113|123456|ABC000001|123456|01.01|987654321|VIC|SMITH^JONES|1|000010134|0087654.3|ABC123|VIC|0|39.12312|+141.12345|020348|000000|<CR><LF>

AF.11 IVU Data Record storage capability

AF.11.1 The IVU shall be capable of storing at least 2000 SD (Detail) and SD (Work) Records.

Note: SD (Detail) and SD (Work) record storage requirements are based on approximately 14 days of operation and 40 SD (Detail) and 100 SD (Work) Records being produced per day.

AF.12 DRD Data Record storage capability

AF.12.1 The DRD shall be capable of storing a minimum of three years of SD (Detail) and SD (Work) Records in plain text.

Note: Based on the assumption of approximately 40 SD (Detail) and 100 SD (Work) Records per day of operation, it is expected that the required size of the DRD would be less than 100Mb.

AF.12.2 The DRD shall not delete or overwrite any records.

AF.12.3 The IVU shall warn the Driver when 95% of the memory in the DRD has been used.

AF.13 DRD Data security

AF.13.1 Each EWD data file shall have an accompanying EWD signature file.

AF.13.2 The name of the EWD signature file shall be derived from the name of the EWD data file by replacing the ".csv" file extension with a ".p7s.b64" file extension.

Note: For example, an EWD data file "abcd.csv" shall have an EWD signature file named "abcd.p7s.b64".

AF.13.3 The EWD signature file shall contain a BASE64 encoded cryptographic Message Syntax (CMS) digital signature for the entire EWD data file:

- d. The digital signature shall not include the signed data
- e. The digital signature shall be formed using the SHA-1 message digest algorithm
- f. The digital signature shall include the full certificate chain for the signer's PKI certificate.

AF.13.4 The EWD Provider shall be responsible for the management of the private key.

AF.13.5 The EWD Provider shall document the key management process to the satisfaction of the System Manager.

Authentication

AF.14 Authentication

AF.14.1 The IVU shall incorporate, subject to the approval of the System Manager, a method of driver identification and authentication based upon the NeAF methodology.

AF.14.2 The identification and authentication methodology shall provide at least a NeAF assurance level 3.

AF.15 Functionality indicator

AF.15.1 The IVU shall contain a visual indication that the IVU is functioning properly.

AF.15.2 The IVU shall contain a visual indication that the IVU is not functioning properly.

AF.16 Printer

AF.16.1 The IVU shall be connected to a printer.

AF.16.2 The IVU shall be able to accept a date range within and inclusive of the last 28 days.

AF.16.3 The IVU shall be able to print one or many days according to the date range entered.

AF.16.4 The contents of the printout shall be as contained within AF.7.3 and AF.7.4.

Note: the font, style or size of the print out may be proposed by the Service Provider. The order of the information and what must be contained are mandatory.

Part B – Specification for EWD Provider

IVU Installation, operation and maintenance

B.1 Type-approved IVUs*

B.2 Installation of IVUs*

B.3 Operation of IVUs*

B.4 Maintenance of IVUs*

B.5 Documentation (managing IVUs) *

Self Declaration Input Device (SDID) installation, use and maintenance

B.6 Installation of SDIDs*

B.7 Use of SDIDs*

B.8 Maintenance and replacement of SDIDs*

B.9 Documentation (managing SDIDs) *

EWD Provider system

B.10 EWD Provider System*

B.11 Maintenance and continuity of EWD Provider System*

B.12 Documentation of EWD Provider System*

Data handling

B.13 Data collection*

B.14 Data processing*

B.15 Data testing*

B.16 Ability to backup and archive data*

EWD Provider quality system

B.20 EWD Provider Quality System

B.20.5 The specification, design, development and testing of the IVU and EWD Provider System shall employ an established software engineering methodology subject to the approval of the Certifying Authority.

D.20.6 Such a methodology shall be in accordance with HB 171 and specifically address the design elements the developer will employ to maximise the evidentiary value of electronic records.

Note: AS/NZS 12207 sets out a framework for such a methodology however methodologies which do not follow the philosophy contained in AS/NZS 12207 may also be suitable.

* For an example please refer to the IAP Functional & Technical Specification.

B.21 Internal and external audits for EWD Provider Quality System

B.22 Information security

- B.22.6 The EWD Provider shall be required to implement an Information Security Management System (ISMS) necessary for the on-going operation of the system.
- B.22.7 The ISMS shall provide assurance that the risks to evidentially-significant information will be managed appropriately by the users of the system.
- B.22.8 This ISMS shall be in alignment with AS/NZS 27001 and implement control mechanisms in accordance with AS/NZS 27002. The ISMS shall give specific care and focus to:
- a. driver identification and authentication
 - b. the management of cryptographic elements of the system including hardware, software and keys
 - c. physical and environmental security
 - d. access control, especially access from privileged users and the mechanisms to provide controlled access to functions and information based upon a user's legitimate tasks on a need-to-know basis
 - e. network and communications security
 - f. incident detection and management.

B.23 Data access controls*

B.24 Reporting to System Manager*

EWD quality monitoring station

B.25 EWD Provider Quality Monitoring Station*

B.26 System Manager audit and review*

B.27 IVU audit and review*

B.28 EWD Provider data audit*

EWD Provider restriction on post-certification change

B.30 EWD Provider restriction on post-certification change*

Data handling

BF.1 Data backup and archiving

- BF.1.1 If the EWD Provider is performing the data storage task for the Record Keeper, the EWD Provider shall:
- maintain all records for a minimum of 3 years
 - protect records from deletion or modification for three years
 - must keep the records at the record location so that they are reasonably accessible to an authorised officer or police officer
 - provide access to the Record Keeper to read the records that they are required to keep

* For an example please refer to the IAP Functional & Technical Specification.

- provide a print out to the Record Keeper of their driver's records for any relevant day on which the driver was using an EWD.

BF.1.2 If the EWD Provider is not performing the data storage task for the Record Keeper, the EWD Provider shall maintain all records for a minimum of one year after successful transmission to the Record Keeper.

EWD Registration Process

BF.9 Driver Registration Process

- BF.9.1 Prior to issuing a driver with their identification and authentication method, the EWD Provider shall verify the identity of the driver against their current driver's licence.
- BF.9.2 The EWD Provider shall issue the driver identification and authentication method with the details authenticated by the driver's driving licence.
- BF.9.3 The EWD Provider shall maintain a register of all driver's authorised to use the identification and authentication method.
- BF.9.4 The EWD Provider shall maintain records concerning the authorisation process including who the officer performing the authorisation was.
- BF.9.5 The EWD Provider shall implement a de-authorisation process through which a driver's authority to access the system will be revoked.
- BF.9.6 Upon de-authorisation, the EWD Provider shall remove the ability of the authentication credentials allocated to the driver to enable access to the EWD System.
- BF.9.7 The EWD Provider shall maintain a register of all drivers that are no longer authorised to use the identification and authentication method for a period of one year after the cancellation of authorisation of this method.

Provision of Records to the Record Keeper

BF.10 Provision of Records to the Record Keeper

- BF.10.1 If the EWD Provider is not providing the data storage task for the Record Keeper, the EWD Provider shall provide a driver's SD (Detail) and SD (Work) Records within 21 days of their declaration

Part C – Specification for Self Declaration Input Device (SDID)

Self Declaration Input Device

C.1 Self Declaration Input Device (SDID) *

C.2 SDID data entry prompt*

C.3 Non-regulatory applications in SDID*

C.4 SD data*

C.6 SD Comments*

C.7 SDID provision to support IVU type-approval*

* For an example please refer to the IAP Functional & Technical Specification.

APPENDIX C – NTC POSITION ON HEAVY VEHICLE SPEED MONITORING

This is the NTC's position on heavy vehicle speed monitoring. This specification has a few major inconsistencies with the EWD Specification (Appendix B):

1. GPS is required to automatically capture Speed Records.
2. The IVU is required to be tethered to the vehicle.
3. Tamper monitoring is required.
4. A printer is not required.

It should be noted that this specification does not include any exceptional reporting, it is merely for a speed recording system.

This specification contains three parts: In-Vehicle Unit (IVU), EWD Provider System, and Self Declaration Input Device (SDID).

The numbering in this Appendix follows the numbering in the Specified EWD (Appendix A) for easy reference.

Part A – Specification for In-Vehicle Unit (IVU)

Physical and environmental characteristics

A.1 In-Vehicle Unit (IVU)

- A.1.1 The EWD Provider shall provide an In Vehicle Unit (IVU) that collects, monitors and stores Global Positioning System (GPS) and other data and transfers that data via a communications device to the EWD Provider.
- A.1.2 An IVU shall be inclusive of:
 - a. a GPS receiver
 - b. a communications device
 - c. all cabling, connections and fixings.
- A.1.3 Other forms of Global Navigation Satellite System can be proposed and adopted by an EWD Provider subject to the approval of System Manager.
- A.1.4 An IVU shall be robustly connected to the respective prime mover/rigid truck.

A.2 IVU GPS capability

- A.2.1 The IVU GPS receiver and GPS antenna shall comply with the all relevant requirements from Australian Communications Authority (the Class Licence).

A.3 Documentation (for IVU)

- A.3.1 The EWD Provider shall document, to the satisfaction of the System Manager, the IVU and all components, cabling and their interfaces.

A.4 IVU identifier

- A.4.1 Each IVU shall have a unique alphanumeric identifier (IVU ID) that will be used to identify:
 - a. the particular IVU
 - b. data from that IVU, when being processed or stored by the EWD Provider System.

A.4.2 The IVU ID shall be visibly marked on the outside casing of the unit as well be stored in the non-volatile programmable read-only memory of the IVU.

A.5 Security

A.5.1 The IVU shall be protected to ensure detection of any unauthorised removal or opening of the IVU.

A.6 Self Declaration capability

A.6.1 The IVU shall be capable of accepting input from a Self Declaration Input Device (SDID) installed by the EWD Provider.

A.7 Suitability for use in vehicles

A.7.1 The EWD Provider shall provide to the System Manager, evidence of compliance from an appropriate body to demonstrate the suitability for use in vehicles for the IVU and all associated components.

A.8 Non-regulatory functionality in the IVU

- A.8.1 It shall be permissible, subject to the approval of System Manager from the perspective of preservation of the integrity of the regulatory application(s), for non-regulatory functionality to be accommodated within the IVU.
- A.8.2 The EWD Provider shall document, to the satisfaction of the System Manager, any non-regulatory functionality to be provided by the IVU.
- A.8.3 The regulatory functionality shall be isolated from any non-regulatory functionality that may be provided by the IVU such that the performance of the IVU for regulatory purposes is not hindered or degraded below the requirements in this Specification, and such that the regulatory application(s) is not compromised.
- A.8.4 The EWD Provider shall document, to the satisfaction of the System Manager, the design features of the IVU which isolate and protect regulatory functionality from any non-regulatory functionality.

Data collection and record generation

A.9 Data

- A.9.1 The IVU shall collect the following data:
 - a. GPS quality data (refer A.10)
 - b. date and time data (refer A.11)
 - c. vehicle position data (refer A.12)
 - d. vehicle direction of travel data (refer A.13)
 - e. vehicle speed data (refer A.14)
 - f. Odometer data (refer A.16)
 - g. alarm status data (refer A.15)
 - h. Self Declaration (SD) data (if applicable) (refer A.17).
- A.9.2 The IVU shall process the collected data to produce the following IVU Data Records which are stored for later transmission:
 - a. Location Records (refer A.18)
 - b. Speed Records (refer A.19)
 - c. Alarm Records (refer A.20)
 - d. SD Records (refer A.21).

A.10 GPS quality data

A.10.1 GPS quality shall be measured to the satisfaction of the System Manager.

A.11 Date and time data

A.11.1 The IVU shall collect and store date and time data in the format defined by the System Manager.

A.11.2 The date and time shall be stored with a resolution of 1 second.

A.11.3 The IVU shall have an internal clock that operates independently of the supporting external power supply.

A.12 Vehicle position data

A.12.1 The IVU GPS receiver shall determine latitude/longitude position of the vehicle.

A.12.2 The latitude/longitude position calculated by the IVU GPS receiver shall not deviate by more than the standard US Department of Defence Accuracy for the absolute horizontal position Australia wide.

A.14 Vehicle speed data

A.14.1 The GPS reported vehicle speed greater than 60 km/h shall be accurate to within 3.0 km/h for 99.9% of the measurements.

A.17 Self Declaration (SD) data

A.17.1 The IVU shall have the capability of receiving, confirming receipt of and storing SD data only from a Self Declaration Input Device (SDID) connected to it.

A.19 Speed Records

A.19.1 The IVU shall be capable of determining a measurement of the speed of the vehicle.

A.19.2 The IVU shall, while the vehicle is in operation, generate Speed Record at periodic time intervals.

A.19.3 A Speed Record shall consist of at least the following data:

- a. record number
- b. date / time of generation (UTC format)
- c. vehicle position
- d. vehicle speed
- e. GPS quality.

A.21 SD Records

A.21.1 The IVU shall generate SD Records from the SD data entered.

A.22 Record numbering

A.22.1 Location, Alarm and SD Records shall be assigned record numbers from the one record numbering sequence, with consecutive and increasing record numbers assigned to successive IVU Data Records in order of generation.

A.22.2 Speed Records shall be assigned record numbers from a separate numbering sequence, with consecutive and increasing record numbers assigned to successive Speed Records in order of generation.

Storage, display and transfer

A.23 IVU Data Record storage capability

A.23.1 The IVU shall be capable of storing at least 20,000 Location, Alarm and SD Records (combined) and at least 200,000 Speed Records.

A.24 IVU external power supply failure/shutdown

A.24.1 In the event that the external power supply supporting the IVU fails or shuts down, the IVU shall be capable of retaining stored data and monitoring the status of the movement sensors for a period defined by the System Manager.

A.25 Data security and confidentiality measures

A.25.1 It shall not be possible for collected or stored data or software memory within the IVU to be accessible or capable of being manipulated by any person, device or system (including the SDID), other than that authorised by the EWD Provider.

A.26 IVU communication capability

A.26.1 The IVU shall be capable of communicating with the EWD Provider from at least the areas nominated by the EWD Provider.

A.26.2 The channel for the transmission of IVU Data Records to the EWD Provider shall be secure and guarantee standards for privacy and data integrity to the level defined by the System Manager.

A.27 Transfer of data from IVU to EWD Provider

A.27.1 The transfer of stored data from the IVU to the EWD Provider shall be performed at least once every 24 hours provided that the IVU is in the communication coverage area offered by the EWD Provider and the vehicle is in operation.

A.27.2 IVU Data Records stored in the IVU shall only be deleted after such data is transferred from the IVU and successful receipt is confirmed by the EWD Provider.

A.28 IVU Data Records and Data Blocks

A.28.1 IVU Data Records shall be transferred from the IVU to the EWD Provider.

A.28.2 Every transfer shall include framing data that identifies its sequential order, IVU ID, version number of IVU component plus software and ability to decode or decompress data.

A.29 Integrity and origin of Data Blocks and IVU Data Records

A.29.1 The numbering shall be sequential.

A.29.2 Each transfer shall contain error detection and error correction coding that operates successfully.

A.29.3 Each transfer shall support a form of data authentication (i.e. some form of message authentication only known and accessible to the EWD Provider), subject to the approval of the System Manager, that can prove the origin and integrity of the IVU Data Records.

A.29.4 The EWD Provider shall document, to the satisfaction of the System Manager, the transfer authentication mechanism.

A.30 Integrity and origin of SD Data

A.30.1 Similar to the integrity of the communication channel between the IVU and the EWD Provider, the SDID should ensure that there is integrity, confidentiality and authenticity of the driver declaration data.

A.31 IVU approval

A.31.1 To facilitate IVU approval testing, multiple IVUs shall be provided to the System Manager.

Data collection and record generation

AS.1 Speed Records

AS.1.1 The collection and storage of Speed Records shall be configurable (on/off) by the EWD Provider and based upon instruction of the Authority.

AS.1.2 Speed Records shall contain the additional fields of:

- a. driver's Licence number
- b. driver's Licence Issuing Jurisdiction
- c. driver's name.

AS.1.3 The population of these fields shall be based upon the information acquired from the identification and authentication method provided by the EWD Provider.

Storage, display and transfer

AS.2 IVU Data Record Storage Capability

AS.2.1 The IVU shall be capable of storing at least 400,000 Speed Records.

Note: These storage requirements are based on approximately 14 days of 24 hour operation

Authentication

AS.3 Authentication

AS.3.1 The IVU shall incorporate, subject to the approval of the System Manager, a method of driver Identification and Authentication based upon the NeAF methodology.

AS.3.2 The Identification and Authentication methodology shall provide at least a NeAF assurance level 3.

Part B – Specification for EWD Provider

IVU Installation, operation and maintenance

B.1 Type-approved IVUs*

B.2 Installation of IVUs*

B.3 Operation of IVUs*

B.4 Maintenance of IVUs*

B.5 Documentation (managing IVUs)*

Self Declaration Input Device (SDID) installation, use and maintenance

B.6 Installation of SDIDs*

B.7 Use of SDIDs*

B.8 Maintenance and replacement of SDIDs*

B.9 Documentation (managing SDIDs)*

EWD Provider system

B.10 EWD Provider System*

B.11 Maintenance and continuity of EWD Provider System*

B.12 Documentation of EWD Provider System*

* For an example please refer to the IAP Functional & Technical Specification.

Data handling

B.13 Data collection*

B.14 Data processing*

B.15 Data testing*

B.16 Ability to backup and archive data*

EWD quality system

B.20 EWD Provider Quality System

B.20.5 The specification, design, development and testing of the IVU and EWD Provider System shall employ an established software engineering methodology subject to the approval of the System Manager.

B.20.6 Such a methodology shall be in accordance with HB 171 and specifically address the design elements the developer will employ to maximise the evidentiary value of electronic records.

Note: AS/NZS 12207 sets out a framework for such a methodology however methodologies which do not follow the philosophy contained in AS/NZS 12207 may also be suitable.

B.21 Internal and external audits for EWD Provider Quality System*

B.22 Information security

B.22.6 The EWD Provider shall be required to implement an Information Security Management System (ISMS) necessary for the on-going operation of the system.

B.22.7 The ISMS shall provide assurance that the risks to evidentially-significant information will be managed appropriately by the users of the system.

B.22.8 This ISMS shall be in alignment with AS/NZS 27001 and implement control mechanisms in accordance with AS/NZS 27002. The ISMS shall give specific care and focus to:

- a. driver identification and authentication
- b. the management of cryptographic elements of the system including hardware, software and keys
- c. physical and environmental security
- d. access control, especially access from privileged users and the mechanisms to provide controlled access to functions and information based upon a user's legitimate tasks on a need-to-know basis
- e. network and communications security
- f. incident detection and management.

B.23 Data access controls*

B.24 Reporting to the System Manager*

EWD Quality Monitoring Station

B.25 EWD Provider Quality Monitoring Station*

* For an example please refer to the IAP Functional & Technical Specification.

B.26 System Manager audit and review*

B.27 IVU audit and review*

B.28 EWD Provider data audit*

B.29 Position audit*

EWD Provider restriction on post-certification change

B.30 EWD Provider restriction on post-certification change*

Part C – Specification for Self Declaration Input Device (SDID)

Self Declaration Input Device

C.1 Self Declaration Input Device (SDID)*

C.2 SDID data entry prompt*

C.3 Non-regulatory applications in SDID*

C.4 SD data*

C.6 SD Comments*

C.7 SDID provision to support IVU type-approval*

* For an example please refer to the IAP Functional & Technical Specification.

TERM & DEFINITIONS

Acronym	Meaning
AFM	Advance Fatigue Management
ATC	Australian Transport Council
BFM	Basic Fatigue Management
CoR	Chain of Responsibility
EWD	Electronic Work Diary
GNSS	Global Navigation Satellite System
HVDF	Heavy Vehicle Driver Fatigue
IVU	In-Vehicle Unit
WWD	Written Work Diary

INFORMATION RETRIEVAL

Austroads (2010), **Performance-based specification for electronic work diary and heavy vehicle speed monitoring (Draft for Public Comment)**, Sydney, A4, 117pp, AP-T170/10

KEYWORDS:

Fatigue, speed, heavy vehicle, electronic work diary, written work diary, enforcement, compliance, intelligent transport systems, specification, trucks, driver identity, certification, auditing, security, freight vehicles, monitoring, intelligent access program, telematics, information communication technologies, work, rest, heavy vehicle driver fatigue legislation, digital tachograph, service providers, fatigue advisory panel.

ABSTRACT:

This report provides the draft specification for an electronic work diary for fatigue monitoring and speed management. The report provides a background to the development of the specification, the philosophy and context of the current written work diary and proposed future environment for an electronic work diary before the specifications are presented. This report was originally delivered to Austroads in November 2009. It contains the full details of a device which meets the terms of the Austroads contract with TCA, and includes requirements for a sustainable telematics platform suitable for possible future extended regulatory use. In doing so, some requirements that add greater integrity to the system extend beyond the policy position being recommended by National Transport Commission (NTC).

The Specification documents comprises of three specifications, (i) Specification for Electronic Work Diary and Heavy Vehicle Speed, (ii) NTC's Position on EWD, and (iii) NTC's Position on Heavy Vehicle Speed Monitoring. The differences between the NTC's position and the Specified EWD are unresolved issues for consultation.