Monitoring of the Implementation
of Digital Tachograph
MIDT

EU-MIDT

Plenary

EU-MIDT/PLE/008-2006

Digital Tachograph System

Guidelines on Decommissioning

PREPARED BY: IDT Project
DATE: 24/04/2006
EU-MIDT Plenary – 008-2006

REF : EU-MIDT/PLE/008-2006

EU-MIDT SECRETARIAT DOCUMENT PREPARATION

OPERATION	NAME	ORGANISATION	DATE
PREPARED BY	IDT Project		30/09/2003
CHECKED BY	Marie-Christine BONNAMOUR	Cybele – MIDT Secretariat	24/04/2006
APPROVED BY	Thierry GRANTURCO	Granturco & Partners – MIDT	24/04/2006
ISSUED BY	Secretariat	MIDT	17/05/2006

CHANGE CONTROL LIST

VERSION	DATE	NAME	DESCRIPTION

DEFINING THE STATUS OF DATA PRESENTED TO A WORKSHOP

SUMMARY

The attached tables are intended to provide an overview of the various situations that a workshop may face when presented with a Vehicle Unit that requires repair.

Table 1:

Defining the various conditions in which data are presented to a workshop.

Table 2:

Summary view of files available to a workshop by use of the workshop card

Table 3:

Relationship between the Overview File and the Company Locks (and exactly what data are protected by the Company Locks).

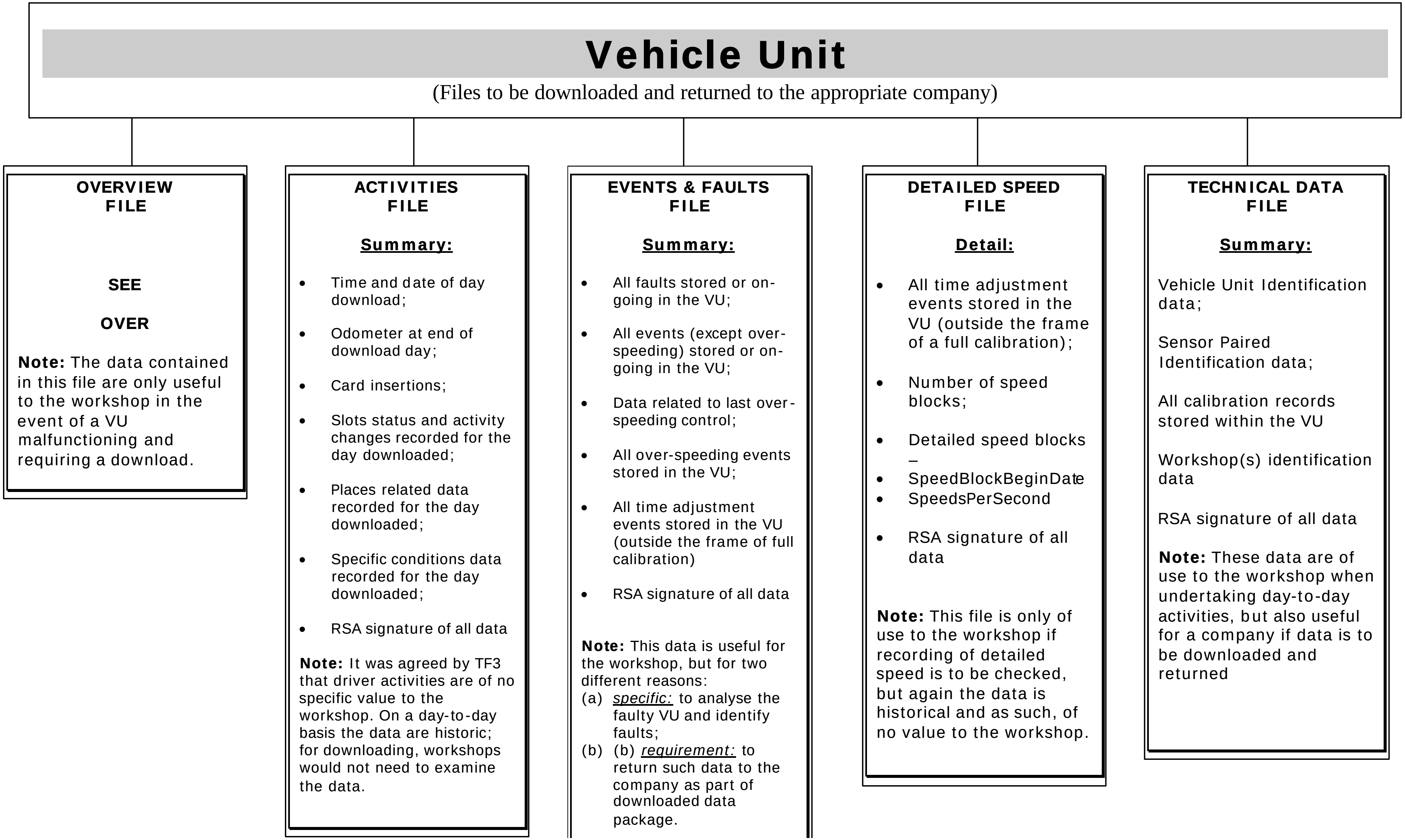
Table 1:

Defining the various conditions in which data are presented to a workshop

Description of Data Identity	Definition	The scope of Data Protection Rules	Responsibility on workshops	Wider Implications
1. Unidentified data	This is data which has been recorded by the vehicle unit, but which cannot be ascribed to either an individual driver or a company because neither the driver card nor company card were used.	Because the data is unattributable and ownership cannot be established, the data must fall outside the scope of Data Protection rules. The only indication of who might own the data is contained by the VIN and/or VRM.	No company ID, nor driver ID available to the workshop from the overview file; therefore no requirement to download.	The data is effectively "dead" data that no company will be able to reasonably establish as its own. It will not be possible for a company to claim it as its own, nor would enforcers be able to use it as particularly reliable.
2. Partially Identified (driver) Data	When a driver card has been used, but not in conjunction with a company card.	The use of a driver card will not, in the overview file, be shown to the workshop. Such data, if it exists, will be contained within the company lock-in/-out dates.	Without being able to identify the company lock-in/-out, workshops are not required to download data.	The data created in the VU (in the scenario where a driver card has been used) will also be available on the driver card, and the driver (and operator) have a responsibility to provide records on request.
3. Partially identified (company) data	When a company card has been used to lock-in data, but no driver card has been used.	Even though no driver card was used, the workshop will not be able to establish this without searching further through the electronic files. There is no requirement to do this.	Company lock-in ID needs to correspond with presented company ID before a workshop downloads.	The absence of a driver card within company lock-in data will only become apparent to either an inspecting officer, or at the point of normal data analysis, both at a later date.
4. Historic, but fully identifiable personal and company data	This is data recorded from a driver card and secured by use of a company card, but which is not the most recent data recorded at time of VU malfunction. It is therefore, historic.	This scenario conforms to all the requirements needed to protect the data from unauthorised access, by correct use of the company card. However, the data are, from a workshop perspective, "historic" and do not represent the most recent record made by the VU at the point of malfunction.	Workshops should retain a copy of this data for a year and release a copy of it only on request (in writing) to the appropriate (identifiable) company. At the end of the one year period, the data should be destroyed.	The retention of such data by a workshops enables a company access to a full set of data which it might not have had the opportunity to download earlier. In genuine cases this will assist operators to maintain full records. It is not, however, nor should it be, regarded as a direct source of enforcement data, or an opportunity for operators to "lose" data.
5. The most recent fully identifiable personal company data	This is data recorded from a driver card and secured by use of a company card, **and** which is the most data recorded at the time of VU malfunction.	This scenario conforms to all the requirements needed to protect the data from unauthorised access, by correct use of the company card. It is also the most relevant data to download as it was in recording mode when the VU malfunctioned.	As above – companies requesting such data must identify themselves and make the request in writing.	This is the ideal situation where full data can be returned to a company in order for them to maintain a continuous record of driver and vehicle activities.
6. Individual, single person operated companies	Sole entities who use a driver card but, because they do not share the vehicle, or in any way "dispose" of it, do not feel obliged to carry or use a Company Card.	A Legal Person (that is, a person who is both an individual and a company too) will not be able to access their own data unless they have (and use) a company card. Therefore the onus should be on that individual to have a company card, thereby conforming to the spirit of the requirement.	For a workshop, the approach should be the same as in No 2, in that it is not for the workshop to decide if a driver is a company too, but visa versa.	Companies are required to provide full records when requested to do so. So, when enforcers visit the home of a sole entity, are they there to look at company records or an individual's records? Once the distinction is made, the problem will probably become less difficult to manage.
7. No data available at all.	This covers occasions when data cannot be downloaded from the VU by a workshop.	Are there any DP issues here, for data that is patently inaccessible? No.	A workshop has to produce a certificate of undownloadability (req261). As good house-keeping, workshops should notify	Complete loss of a minimum of 365 days worth of data from a vehicle. The problem may (will) arise that if a company in scenario No 3, 4 or 5 requires a copy of its data, (a) it will not be able to get it and, (b) no one will be able to prove that

			the competent authorities of the VU that was undownloadable and the vehicle from which it came.	that data was actually in the vehicle unit that is undownloadable.

Table 2:
Files Available to the Workshop by use of a Workshop Card
(As defined on pages 160-163 of Appendix 7 of Annex 1B)



Vehicle Unit

(Files to be downloaded and returned to the appropriate company)

OVERVIEW FILE

SEE

OVER

Note: The data contained in this file are only useful to the workshop in the event of a VU malfunctioning and requiring a download.

ACTIVITIES FILE

Summary:

- Time and date of day download;
- Odometer at end of download day;
- Card insertions;
- Slots status and activity changes recorded for the day downloaded;
- Places related data recorded for the day downloaded;
- Specific conditions data recorded for the day downloaded;
- RSA signature of all data

Note: It was agreed by TF3 that driver activities are of no specific value to the workshop. On a day-to-day basis the data are historic; for downloading, workshops would not need to examine the data.

EVENTS & FAULTS FILE

Summary:

- All faults stored or on-going in the VU;
- All events (except over-speeding) stored or on-going in the VU;
- Data related to last over-speeding control;
- All over-speeding events stored in the VU;
- All time adjustment events stored in the VU (outside the frame of full calibration)
- RSA signature of all data

Note: This data is useful for the workshop, but for two different reasons:
(a) *specific:* to analyse the faulty VU and identify faults;
(b) (b) *requirement:* to return such data to the company as part of downloaded data package.

DETAILED SPEED FILE

Detail:

- All time adjustment events stored in the VU (outside the frame of a full calibration);
- Number of speed blocks;
- Detailed speed blocks –
- SpeedBlockBeginDate
- SpeedsPerSecond
- RSA signature of all data

Note: This file is only of use to the workshop if recording of detailed speed is to be checked, but again the data is historical and as such, of no value to the workshop.

TECHNICAL DATA FILE

Summary:

Vehicle Unit Identification data;

Sensor Paired Identification data;

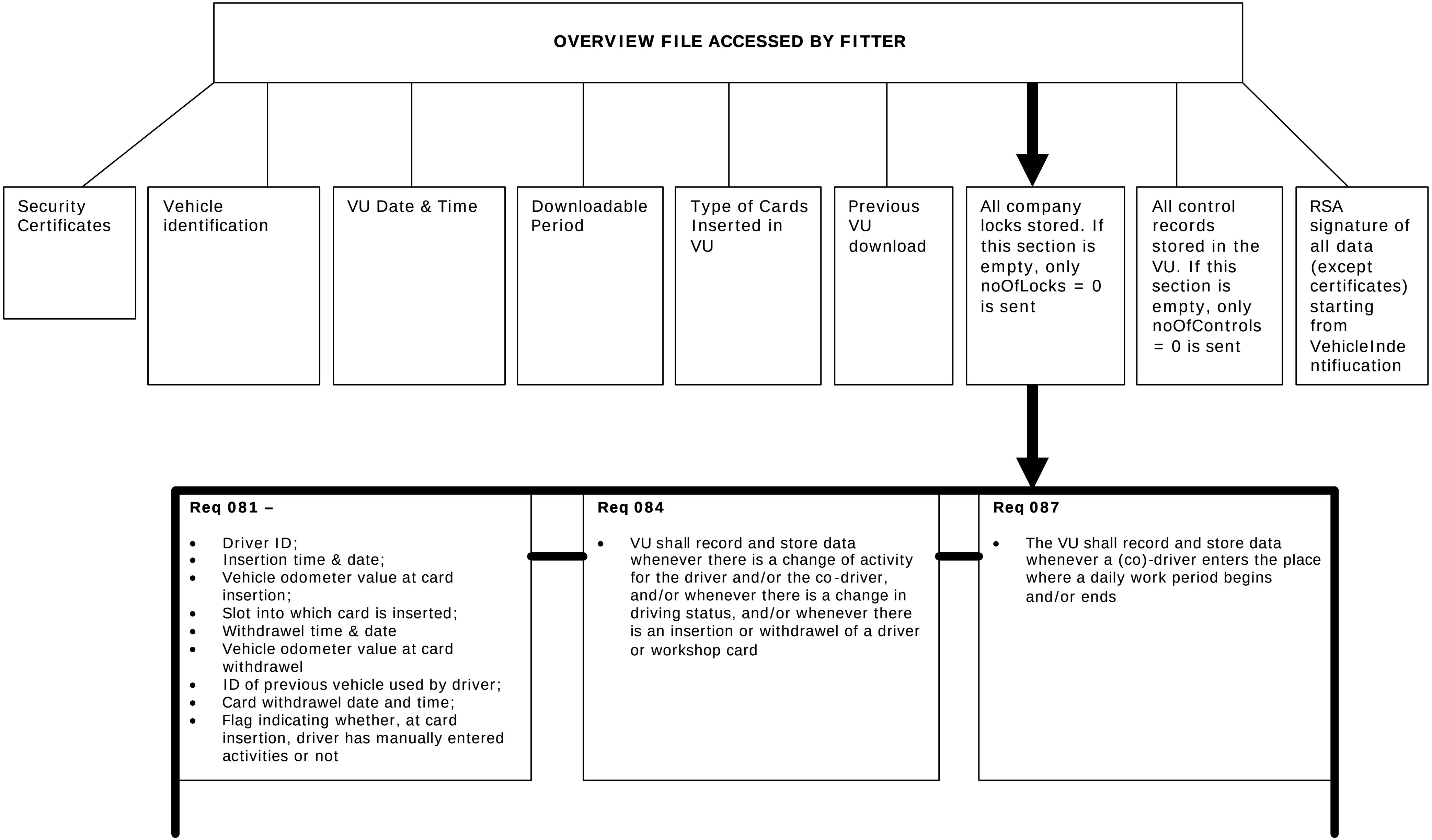
All calibration records stored within the VU

Workshop(s) identification data

RSA signature of all data

Note: These data are of use to the workshop when undertaking day-to-day activities, but also useful for a company if data is to be downloaded and returned

Table 3:
Diagram of the relationship between the Overview File and Company Locks



OVERVIEW FILE ACCESSED BY FITTER

Security Certificates

Vehicle identification

VU Date & Time

Downloadable Period

Type of Cards Inserted in VU

Previous VU download

All company locks stored. If this section is empty, only noOfLocks = 0 is sent

All control records stored in the VU. If this section is empty, only noOfControls = 0 is sent

RSA signature of all data (except certificates) starting from VehicleIndentifiucation

Req 081 –

- Driver ID;
- Insertion time & date;
- Vehicle odometer value at card insertion;
- Slot into which card is inserted;
- Withdrawel time & date
- Vehicle odometer value at card withdrawel
- ID of previous vehicle used by driver;
- Card withdrawel date and time;
- Flag indicating whether, at card insertion, driver has manually entered activities or not

Req 084

- VU shall record and store data whenever there is a change of activity for the driver and/or the co-driver, and/or whenever there is a change in driving status, and/or whenever there is an insertion or withdrawel of a driver or workshop card

Req 087

- The VU shall record and store data whenever a (co)-driver enters the place where a daily work period begins and/or ends

Unsecured “open” data which would also be available to the company, between the two points of locking in and locking out			
Activities File	**Events & Faults File**	**Detailed Speed File**	**Technical Data File**