



FMCSA-2004-18940-2

Federal Motor Carrier Safety Administration

Office of Business and Truck Standards and Operations

Hours of Service (HOS) Research and Analysis Modules

Module 1 - HOS Data Record Structure and Data Security

**Module 2 - Engine Control Module and Transmission
Control Module Usage for HOS Solutions**

Module 3 - Geo-Referenced Data in HOS Solutions

Module 4 - Paper Backup System for HOS Solutions

**Module 5 - High-Level Architectures for EOBR HOS
Solutions**

January 21, 2003



Federal Motor Carrier Safety Administration

Office of Business and Truck Standards and Operations

Research and Analysis on Hours of Service (HOS) Data Record Structure and Data Security

January 21, 2003



Hours of Service (HOS) Data Record Structure and Data Security

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
TABLE OF CONTENTS.....	II
SECTION 1 – EXECUTIVE SUMMARY.....	1
SECTION 2 - IMPORTANCE OF A COMMON HOS DATA STANDARD.....	2
SECTION 3 – REQUIRED HOS DATA ITEMS	3
3.1 HOS Metadata	3
3.2 Mapping to the FMCSA Regulation Section 395.15	4
3.3 Notional Data Record Structure	5
3.3.1 Storing Text Data - The ASCII and UNICODE Character Sets	6
3.3.2 Storing Numeric Data – Integer and Floating Point Encoding	9
3.3.3 A Notional 24 Byte HOS Data Record	11
3.4 Media Limitations	12
3.4.1 Portable Media	12
3.4.2 Fixed Media.....	13
SECTION 4 – DATA SECURITY	16
4.1 Data Security Basics.....	16
4.2 Trusted Data	17
4.2.1 Secret-Key Cryptography.....	17
4.2.2 Public-Key Cryptography.....	17
4.2.3 Digital Envelopes	18
4.2.4 Key Management	18
4.2.5 The Escrowed Encryption Standard	18
4.3 Authenticated Data	20
4.4 Secure Data.....	21
4.4.1 The Data Encryption Standard (DES)	21
4.4.2 The Advanced Encryption Standard (AES)	22
4.4.3 HOS Applicability	22
4.5 Relevant U.S. Government Standards.....	22
4.5.1 FIPS 46-3 – Data Encryption Standard	23
4.5.2 FIPS 185 – Escrowed Encryption Standard	24
4.5.3 FIPS 186-2 – Digital Signature Standard.....	25
4.5.4 FIPS 196 - Entity Authentication Using Public Key Cryptography	25
4.5.5 FIPS 197 – Advanced Encryption Standard.....	26
SECTION 5 - RECOMMENDATIONS.....	27
BIBLIOGRAPHY	30



Hours of Service (HOS) Data Record Structure and Data Security

SECTION 1 – EXECUTIVE SUMMARY

A standardized and compact Hours of Service (HOS) data record can be constructed to span the expected range of IT technology that will be used for HOS solutions. Initial analysis indicates that a 24 character record that contains the information required by FMCSA Regulation Section 395.15 is feasible. This record could store the date, time, odometer reading, and latitude/longitude when a driver status changes or State Border Crossing (SBC) event takes place.

A lowest common denominator solution using an inexpensive 64KB capacity SmartCard and 20 KB of pre-loaded data would be able to store between 1500 and 2000 24 character records, the research and analysis for this study indicates that would be sufficient a SmartCard would have sufficient memory storage for a single trip. SmartCards are also available with “on the chip” Java Virtual Machines that can handle the encryption in the “front-end” system.

Vehicle engine control and/or transmission control modules can provide primary and backup timestamp, odometer, and moving/not moving portions of the data record based on initial analysis of the SAE J1708 and J1587 built-in messages. The use of the ECM in general will be described in detail in the next report “Research and Analysis on ECM/TCM Usage for HOS Solutions.”

This analysis has determined that numeric codes can be used for both Place Names (PN) and SBC locations. This minimizes data record size and allows direct code look-up when a GPS system provides the latitude and longitude of the event discretely. When there is no GPS system the driver can use the same lookup data to quickly extract the code. The use of codes for PNs and SBCs will be described in detail in the “Research and Analysis on Place Names in HOS Solutions” and “Research and Analysis on State Border Crossing in HOS Solutions” whose write-ups are also in work now.

The FIPS standards referenced in Section 3.5 provide the guidance for a fully adequate system to secure the HOS data. Almost all the processes called out in these standards are available as commercial off-the-shelf (COTS) products which will minimize the time and expense of fielding a HOS solution.

“Back-end” solutions can all be accomplished on PC’s without the need for high-end and expensive servers in any but the largest carriers. This will allow the individual and small operation, which makes up the bulk of the trucking industry, to be HOS compliant with a simple desktop, laptop, or personal computer (PC).

Adequate data security is accomplished by assuring that the data is encrypted to the media once and not modified thereafter. Error and the re-entry of corrected data is written to the media, providing an audit trail. This makes the data “trusted” and minimizes the possibility of direct tampering during the trip.

The same encryption spans the archival function in the “back-end” system after the trip is over with secure logs appended to the trip record to track who accesses the data over time. This completes the audit process, resulting in an “end-to-end” audit trail for the data. These end-to-



Hours of Service (HOS) Data Record Structure and Data Security

end logs are themselves a deterrent to tampering as authentication using digital signatures would be used to log when and who is accessing the data. CD-ROMS, which cannot be edited, should be used to archive the data.

SECTION 2 - IMPORTANCE OF A COMMON HOS DATA STANDARD

Future HOS solutions that will eventually make their way into the marketplace will naturally utilize a wide variety of Information Technology (IT) techniques in their attendant hardware and software. Most of this variation will occur in the “front-end” portion of the overall HOS solution. The “font-end” portion of the solution is defined as the hardware and software used by the vehicle operators.

These solutions range from the required paper backup system to easy-to-use firmware-centric systems with a portable storage device (SmartCard, Contact Memory Button, etc.) to more complex stand-alone computers like PalmOS, PocketPC, Personal Data Assistants (PDA's) that would be docked in the truck, and Personal Computers (PC's) to gather and process the HOS data.

After the data has been gathered the “back-end” portion of the HOS solution, probably a PC-based system, will recover the individual HOS data for each trip and store it. Regardless of the “front-end” system used the data specification for the information that encompasses the HOS data needs a common specification. Section 2 of this document depicts a recommended HOS data structure and its utilization across the spectrum of expected storage media.

This common data specification will assure that the “front-end” and “back-end” solutions will have a common interface for collecting the HOS data and processing it. More importantly, the HOS solutions are desired to be as tamper-proof as is practically possible so as to gather accurate data during normal operations. The common data standard also needs to directly address data security.

The data needs to be secured effectively within the various HOS solutions to allow the operator to easily enter the data, thereafter storing it in an encrypted fashion to largely eliminate tampering. The data can be easily entered by authenticated sources with any editing tracked with additional records to form an audit trail for the HOS information. Automated cryptography, is covered in Section 3 of the document. This section provides high-level tutorial about the currently employed U.S. Government (USG). Approved methods as well as other commercial practices, focused on their application to the HOS problem.

Lastly, Section 5 of the document provides Conclusions and Recommendation for the envisioned common data standard.



SECTION 3 – REQUIRED HOS DATA ITEMS

3.1 HOS Metadata

Metadata is a database term that essentially means “data about data”. It is simply information about multiple data items within the context of the entire set of data. Typical databases have multiple tables with each table containing multiple columns and each column containing unique datum’s, commonly called fields of data, in rows. The subject of each column aggregately forms the metadata for the table.

The metadata for the entire database is simply the aggregate of the description of what each table holds. The HOS service problem is easy to bounded for metadata as 395.15 relates specific Electronic On Board Recorder (EOBR) requirements for an automated solutions. Specifically Section 395.15(c) breaks out 13 specific metadata items with 395.15(d)(1,2) aggregately providing the need for the location to be gathered when HOS duty status changes or a State border is crossed. Since the location data can be either demanded (if GPS is available) or input (if no GPS is available) listed as 2 metadata items.

This totals to 15 metadata items for a minimal HOS solution to gather. Some of this data can be **Pre-loaded** as they are not Duty Status dependent. This includes things like the Vehicle’s identifying number, Carrier Name, Main Office Address, and so on. This data would be loaded before the beginning of the trip and would not need time and location information as Duty Status changes. This information would also be secure as the key used to encrypt the Duty Status change and State Border Crossings would be formed and stored on the device when the pre-loading activity takes place. This report’s analysis recommends that the data needed to authenticate the originator of the preload be located here.

To minimize tampering a HOS Solution should obtain discrete date-time and location information for external sources. Whenever a Duty Status change or State Border Crossing occurs we want to **demand** this information, logging it as a part of the HOS data record automatically to virtually eliminate tampering. The date-time data can be demanded directly from the Engine Control Module (ECM) of the vehicle as a primary source as well as directly from a Global Positioning Satellite (GPS) component if present. The ECM data may not be absolutely accurate but the differential times used to compute the total hours driven would be. The GPS source is completely external and very accurate, offering the best overall source for date-time information. Any HOS solutions will need to have firmware or software that can automatically detect and get the date-time information from either source. The location data is best obtained from a GPS system which can discretely provide the latitude and longitude of the vehicle as needed.

Other information would be **input** directly that information is the four Duty Status codes and the State Border Crossing event mentioned earlier. The way the surrounding data about when and where the HOS events take place would be gathered in the “front-end” and/or “back-end” portions of the solution. This date-time and location data could be demanded or input, depending on whether the solution can provide location information via a GPS hardware component.



Hours of Service (HOS) Data Record Structure and Data Security

Two of the fifteen items have to be **computed**. These are the Total Miles Driven Today FMCSA Regulation Section (395.15(c) (6)) and Total Hours (395.15(c) (12)) which would be computed based on the time-stamped changes in the duty status.

3.2 Mapping to the FMCSA Regulation Section 395.15

The last section talked about four ways the HOS metadata would be gathered. They are:

- P – Preloaded data that is stored once before the trip starts (6 of the 15 items)
- I – Input by the driver as duty status changes or a state border is crossed (5 of the 15)
- D – Demanded from internal sources, the date-time or location (2 of the 15)
- C – Always computed as the Miles Driven and Total Hours are time depended (2 of the 15)

The sum of the above is 6+5+2+2 or 15. The date-time of an event can probably be demanded from an internal source (ECM, CPU Clock, or GPS unit) while the location, stored as a code, may have to be input. If the particular solution has a GPS receiver built-in both the time and location (latitude and longitude) can be demanded discretely.

If there is no GPS available the time can still be demanded from other sources automatically but the location cannot be. Hence the location metadata item can be either demanded or input depending on the solution's hardware sophistication. Table 1, shown below, depicts the mapping of the 15 items to 395.15. The "type" column has the P, I, C, or D designation.

#	Ref	Type	Description
1	§395.15(c)(1)	I	Status Change - Driver is Off Duty
2	§395.15(c)(2)	I	Status Change - Driver is in Sleeper Berth
3	§395.15(c)(3)	I	Status Change - Driver is On Duty - Not Driving
4	§395.15(c)(4)	I	Status Change - Driver is On Duty - Driving
5	§395.15(c)(5)	D	Date-Time Group
6	§395.15(c)(6)	C	Total Miles Driving Today
7	§395.15(c)(7)	P	Truck/Tractor & Trailer Number
8	§395.15(c)(8)	P	Name of Carrier
9	§395.15(c)(9)	P	Main Office Address
10	§395.15(c)(10)	P	24-hour period starting time
11	§395.15(c)(11)	P	Name of Co-Driver
12	§395.15(c)(12)	C	Total Hours
13	§395.15(c)(13)	P	Shipping Doc Numbers, etc.
14	§395.15(d)(1,2)	D,I	Location – Stored as numeric codes (only requires numeric keypad for data entry versus a keyboard)
15			

Table 1 – 395.15 Metadata Mapping

The items in the table above shows the information needed to encompass HOS but not what the recommended data record would physically contain. The common data standard mentioned



Hours of Service (HOS) Data Record Structure and Data Security

earlier needs to be structured so that regardless of the software used to articulate the data and the media used to securely hold it the results will always be the same.

The computed fields will not show up in the record structure at all as they are computed when needed. Likewise the Pre-loaded data need only be stored once, before the trip starts. The rest of the items revolve around the 2 primary events that will gather HOS information. These are either that the duty status has changed (4 choices on what it has changed to) or that the truck has crossed a state border. In either case the time at which it occurred and the location where it has occurred is discretely needed.

If it is a Duty Status Event (DSE) then the location of the nearest named place is needed, this report recommends that the FIPS 55 codes be exploited for this as they specifically (when prefixed with the FIPS state code), uniquely locate a named place. Initial analysis indicates that a sufficient number of FIPS codes can be stored in the software solutions to either translate a latitude/longitude pair as supplied by a GPS system or step a user through quickly recovering that unique code. The Module 3 report on "Research and Analysis of Place Name Data Sources and Usage" will document this analysis and provide the details.

If it is a SBC then the states to and from, as well as the road being traveled on, is desired. There are no FIPS codes for this but the taxonomy of the unique isolated borders between states can be exploited to quickly translate either a GPS-supplied latitude/longitude pair or user inputs into the code. Initial analysis indicates that this information can easily fit into the various software solutions. The Module 4 report "Research and Analysis of State Border Crossing Data Sources and Usage" will document this analysis and provide the details.

More event types that should be added that can anecdotally capture attempts at tampering as well as DSE's and SBE's entered in error and corrected. These events are concerned with what was re-done and would probably not store the location and place name or border crossing location information as the "Cancel" event should immediately follow the mistaken entry. They would however record the ECM demanded date-time group and odometer reading to provide timing differences which, taken as a pattern, indicate planned tampering with the HOS data records.

The notion is that only the minimum data is stored in an individual Status Change or SBC event is input. This is important as the encryption process is more efficient and the record length is minimized, allowing a long trip to comfortably fit on a low capacity media device like a SmartCard. This also will minimize the archival storage as large numbers of HOS record accumulate over time. The notional data record structure articulated in the next section.

3.3 Notional Data Record Structure

The goal is to develop a common data record structure that will contain the required HOS information. The smaller the number of characters in the record the more efficient the solution in limited media like SmartCards will be not to mention the archival storage requirements. It is important to understand this notion of byte-wise storage as this is central to adequately describing the record structure.



3.3.1 Storing Text Data - The ASCII and UNICODE Character Sets

Computers process binary data, ones and zeros, during processing. Each 0 or 1 takes up a bit of data. Eight bits form a byte of data and the byte is the commonly used unit of measure for data records. HOS data should contain both alphanumeric characters and numbers; and these use specific numbers of bytes as follows:

Alphanumeric Characters – Each character uses a byte of data. All the characters taken together form a “string” and the number of bytes for the whole string using the standard American Standard Code for Information Interchange (ASCII) character set is 1 byte for each character. This was adopted internationally by the International Standards Organization (ISO) as ISO 8859-1. So the number of bytes used is the same as the number of characters stored.

The ASCII character set was developed at the beginning of the computer age to form a common set of characters. There are 128 standard characters, 32 of which are non-printing control characters, the rest being letters, numbers, mathematical symbols, and punctuation marks.

All 8 bits of the single byte are available to describe each character that is 2^8 in base 2 or 256 in base 10, or 256 possible characters. As computer technology progressed the initial 128 characters were not enough and the so-called “extended” ASCII set was adopted to add more arcane mathematical symbols, language specific punctuation, common fractions, commonly used Greek letters, and specialized characters for putting borders around messages – using up the remaining 128 ASCII codes.

More recently used is the UNICODE character set (ISO/IEC 10646) which uses three different encoding paradigms: UTF-8, UTF-16, and UTF-32. The last number of the set indicates the bits used for each character. This allots more bits for each character to encompass specific foreign languages into a single common specification. The UTF-32 specification allows up to 2^{32} or 4.23 Billion characters. This process uses four times the storage.

The UTF-8 part of UNICODE is identical to the ASCII “extended” character set and this analysis recommends that HOS solutions support either ASCII (ISO 8859-1) or UNICODE UTF-8 (ISO/IEC 10646). This will allow the text in the pre-loaded data to contain upper and lower case letters and should be more than sufficient.

Assuming that PC’s will be used in back-end solutions the record should use the standard ASCII 10 (LF) and ASCII 13 (CR) combination of control characters to indicate the end of the record. This will allow the information to be directly viewed in a text editor. This will account for 2 bytes of the record.

Table 2 on the next page contains the 32 control characters with their numeric code numbers in Decimal (Base 10), Hexi-decimal (Base 16), Octal (Base 8), and Binary (Base 2) values. The notes to the right indicate the function. These control codes are invoked by the user with a keyboard as single keys like Escape or Enter, or more commonly as combinations with the Control key. The ASCII 10 and 13 are shown in **bold**.



Hours of Service (HOS) Data Record Structure and Data Security

Dec	Hex	Oct	Bin	Keybd*	Description
0	0	0	000000	^@	NUL (null)
1	1	1	000001	^A	SOH (start of heading)
2	2	2	000010	^B	STX (start of text)
3	3	3	000011	^C	ETX (end of text)
4	4	4	000100	^D	EOT (end of transmission) - Not the same as ETB
5	5	5	000101	^E	ENQ (enquiry)
6	6	6	000110	^F	ACK (acknowledge)
7	7	7	000111	^G	BEL (bell) - Caused teletype machines to ring a bell. Causes a beep in many common terminals and terminal emulation programs.
8	8	10	001000	^H	BS (backspace) - Moves the cursor (or print head) move backwards (left) one space.
9	9	11	001001	^I	TAB (horizontal tab) - Moves the cursor (or print head) right to the next tab stop. The spacing of tab stops is dependent on the output device.
10	A	12	001010	^J	LF (NL line feed, new line) - Moves the cursor/print head to a new line.
11	B	13	001011	^K	VT (vertical tab)
12	C	14	001100	^L	FF (form feed) - Advances paper to the top of the next page when printing.
13	D	15	001101	^M	CR (carriage return) - Moves the cursor all the way to the left, but does not advance to the next line.
14	E	16	001110	^N	SO (shift out) - Switches output device to alternate character set.
15	F	17	001111	^O	SI (shift in) - Switches output device back to default character set.
16	10	20	010000	^P	DLE (data link escape)
17	11	21	010001	^Q	DC1 (device control 1)
18	12	22	010010	^R	DC2 (device control 2)
19	13	23	010011	^S	DC3 (device control 3)
20	14	24	010100	^T	DC4 (device control 4)
21	15	25	010101	^U	NAK (negative acknowledge)
22	16	26	010110	^V	SYN (synchronous idle)
23	17	27	010111	^W	ETB (end of transmission block) - Not the same as EOT
24	18	30	011000	^X	CAN (cancel)
25	19	31	011001	^Y	EM (end of medium)
26	1A	32	011010	^Z	SUB (substitute)
27	1B	33	011011	^[ESC (escape) - The Esc Key
28	1C	34	011100	^\ ^	FS (file separator)
29	1D	35	011101	^] ^	GS (group separator)
30	1E	36	011110	^^	RS (record separator)
31	1F	37	011111	^	US (unit separator)

* The exponentiation Shift-6 symbol denotes pressing the Control Key First

Table 2 – ASCII Control Characters



Hours of Service (HOS) Data Record Structure and Data Security

Table 3, shown below, has the rest of the characters and would be used for the visible characters in the HOS record as displayed to the users of the “front-end” and “back-end” systems.

Dec	Hex	Oct	Bin	Disp	Kbd	Dec	Hex	Oct	Bin	Disp	Kbd	Dec	Hex	Oct	Bin	Disp	Kbd
32	20	40	100000	Blank	Space	64	40	100	1000000	@	@	96	60	140	1100000	,	,
33	21	41	100001	!	!	65	41	101	1000001	A	A	97	61	141	1100001	a	a
34	22	42	100010	"	"	66	42	102	1000010	B	B	98	62	142	1100010	b	b
35	23	43	100011	#	#	67	43	103	1000011	C	C	99	63	143	1100011	c	c
36	24	44	100100	\$	\$	68	44	104	1000100	D	D	100	64	144	1100100	d	d
37	25	45	100101	%	%	69	45	105	1000101	E	E	101	65	145	1100101	e	e
38	26	46	100110	&	&	70	46	106	1000110	F	F	102	66	146	1100110	f	f
39	27	47	100111	,	,	71	47	107	1000111	G	G	103	67	147	1100111	g	g
40	28	50	101000	((72	48	110	1001000	H	H	104	68	150	1101000	h	h
41	29	51	101001))	73	49	111	1001001	I	I	105	69	151	1101001	i	i
42	2A	52	101010	*	*	74	4A	112	1001010	J	J	106	6A	152	1101010	j	j
43	2B	53	101011	+	+	75	4B	113	1001011	K	K	107	6B	153	1101011	k	k
44	2C	54	101100	,	,	76	4C	114	1001100	L	L	108	6C	154	1101100	l	l
45	2D	55	101101	-	-	77	4D	115	1001101	M	M	109	6D	155	1101101	m	m
46	2E	56	101110	.	.	78	4E	116	1001110	N	N	110	6E	156	1101110	n	n
47	2F	57	101111	/	/	79	4F	117	1001111	O	O	111	6F	157	1101111	o	o
48	30	60	110000	0	0	80	50	120	1010000	P	P	112	70	160	1110000	p	p
49	31	61	110001	1	1	81	51	121	1010001	Q	Q	113	71	161	1110001	q	q
50	32	62	110010	2	2	82	52	122	1010010	R	R	114	72	162	1110010	r	r
51	33	63	110011	3	3	83	53	123	1010011	S	S	115	73	163	1110011	s	s
52	34	64	110100	4	4	84	54	124	1010100	T	T	116	74	164	1110100	t	t
53	35	65	110101	5	5	85	55	125	1010101	U	U	117	75	165	1110101	u	u
54	36	66	110110	6	6	86	56	126	1010110	V	V	118	76	166	1110110	v	v
55	37	67	110111	7	7	87	57	127	1010111	W	W	119	77	167	1110111	w	w
56	38	70	111000	8	8	88	58	130	1011000	X	X	120	78	170	1111000	x	x
57	39	71	111001	9	9	89	59	131	1011001	Y	Y	121	79	171	1111001	y	y
58	3A	72	111010	:	:	90	5A	132	1011010	Z	Z	122	7A	172	1111010	z	z
59	3B	73	111011	;	;	91	5B	133	1011011	[[123	7B	173	1111011	{	{
60	3C	74	111100	<	<	92	5C	134	1011100	\	\	124	7C	174	1111100		
61	3D	75	111101	=	=	93	5D	135	1011101]]	125	7D	175	1111101	}	}
62	3E	76	111110	>	>	94	5E	136	1011110	^	^	126	7E	176	1111110	~	~
63	3F	77	111111	?	?	95	5F	137	1011111			127	7F	177	1111111	N/A	Del

Table 3 – ASCII Display Characters

The table above shows that all the required letter and number information that can be entered and encrypted for the HOS solution.

Up to this point only the text part of the data has been addressed. There are more efficient ways of encoding the HOS information as numerical values. Any HOS solution will need to recover and store odometer readings to compute the miles driven, date-time data for time stamping the HOS record, and numeric values for the codes that represent the nearest place or location of a State Border Crossing. The next section covers these ideas.



Hours of Service (HOS) Data Record Structure and Data Security

3.3.2 Storing Numeric Data – Integer and Floating Point Encoding

The HOS dataset has a few numerical records that need to be stored as DSE and BCE's occur during normal operations. These values need to record the date and time, a discrete measure that can be used to compute the miles driven, and location data which will be pairs of latitude and longitude. In addition there will be the codes that represent the nearest named place or specific border crossing.

The analysis assumes that each HOS record will contain:

- (1) An identifier for the DSE or SBC event as a single character
- (2) An identifier for the type of event (the 4 codes for an DSE or blank for a SBC) as a single character
- (3) An identifier for the driver or co-driver as a single character
- (4) An identifier as to whether the vehicle is moving or not moving as a single character
- (5) The date and time of the event to be stored for each event
- (6) The Odometer reading from the vehicle's ECM for miles driven calculations
- (7) The location of the vehicle when the event takes place as a latitude and longitude pair
- (8) A code to represent the nearest place name (for DSE's) or specific crossing (for SBCs)

The first four in the list above are 1 byte characters for a total of 4 bytes.

The rest can be more efficiently stored by using numeric values with standard encodings. Since the "back-end" systems will be PC-based the standard encoding for integer and floating point variables can be directly used. The units of measure need to be evaluated to determine which standard integer or floating point encodings should be used.

HOS data is encrypted to minimize tampering. Most encryption algorithms divide up or parse the data into 64 bit blocks. 64 bits is 8 bytes so it is advantageous to define the HOS record size in multiples of 8 bytes.

It is recommended that units of seconds be used since it is a fixed point in time. Using units of seconds allows the date-time group to be accurate to +/- a second. Using a relatively recent date as the zero referent for the value also means that an integer encoding can be used. There are two encodings; Integer and Long Integer that are available.

The integer encoding will store a value between -32,768 and +32,767 in 2 bytes of space while the long integer will store a value between -2,147,483,648 and +2,147,483,647 in 4 bytes of space. In both cases the positive values is 1 less than the negative to handle storing zero. . In this case 32,767 seconds is the equivalent of less than one day (60 * 60 * 24 or 86,400 seconds) of time, making the Integer encoding unusable for HOS as almost all trips are greater than a day in length.



Hours of Service (HOS) Data Record Structure and Data Security

The long integer encoding measured in units of seconds represents 2,147,483,647/60/60/24/365.25 or approximately 68.05 years that could be measured in the HOS solutions, this duration could be doubled using an unsigned encoding scheme which applies here as negative values of time are nonsequetar. It is unlikely that the HOS record format will remain unchanged for 146 years given the extremely rapid growth in IT technology. It appears that the Long Integer is a viable way to store the date-time group – all in 4 bytes of space. Using characters, even with the delimiter removed in the form “mmddyhhmmss” would use 12 bytes or 3 times as much as using the long integer. This makes 4 bytes for the date-time group.

The odometer reading will measure the miles driven and is typically recovered from the ECM (SAE J1587, message A.245) which is encoded in 4 bytes with a bit resolution of +/- .10 miles. This can be converted to miles using a single precision floating point encoding or just store the 4 bytes returned from the ECM directly and decode as needed. The simplest solution is to just store the 4 bytes directly. This makes 4 bytes for the Oodometer reading.

The location data that is recovered (if a GPS module is available) or input by the user will need to relate the latitude and longitude defining the location. The values for each will generally be recovered in decimal degrees which will generally need 5 or 6 digits in the fractional portion of the number to indicate the location in sufficient accuracy.

The latitude value will vary between +/- 90 degrees north or south while the longitude varies between +/-180 degrees east or west of the Greenwich, England Prime Meridian. This means that the mantissa (the total number of digits in the number) is, as a worst case, 3+6 or 9 digits. The Single and Double Precision floating point encodings are available to store the number directly. Single Precision encoding takes 4 bytes but only provides a 7 place mantissa which is insufficient. The Double Precision encoding provides a 15 place mantissa which is more than enough for this purpose but uses 8 bytes (16 for the lat/lon pair).

Another option is to again make use of the Long Integer encoding which can support a plus or minus 10 digit number. The decimal place can be eliminated with the user input or GPS provided fixed at a 6 place fractional number. For longitudes >100 degree a total of 9 places would be needed and 10 are available. This would allow the location pair to be stored in a total of 8 bytes or ½ of the storage needed with floating point encoding. This case has 8 bytes for the location data.

Lastly, the code for the place name (for DSE's) or border crossing location (for SBE's) needs to be stored. The FIPS 55 state code can have up to 5 digits but are redundant between states. To make the code a unique identifier for a place the state 2 digit FIPS code must be added, so 7 digits are needed. Integer encoding at 2 bytes only offers 5 digits and therefore will not work for the entire string. Long integer encoding at 4 bytes offers 9 digits and will be adequate. Note that keeping the FIPS 55 and state FIPS codes separately stored as integers uses the same storage as a single long integer but is easier to program in the solutions. In this case two 2 byte integers for the FIPS codes makes a total of 4 bytes.



Hours of Service (HOS) Data Record Structure and Data Security

The total for a notional HOS record is 4 bytes for the character portion (1-4 in the list on the last page) + 4 bytes for the date-time group + 4 bytes for the Odometer + 8 bytes for the location data + 4 bytes for the FIPS codes for a total of 24 bytes for each record. The next section shows the specific structure with the columnar ranges and their nomenclature.

3.3.3 A Notional 24 Byte HOS Data Record

Table 4, shown below, shows the structure of the notional record based on the descriptions of the last section. The 24 byte record length also works well with the encryption notion as there would be three 8 byte blocks for the entire record.

Byte Count	1	1	1	1	4	4	4	4	4
Data Type	Char	Char	Char	Char	Long Int	US Lng Int*	Long Int	Long Int	Long Int
Char Pos	01	02	03	04	05 06 07 08	09 10 11 12	13 14 15 16	17 18 19 20	21 22 23 24
Description	Event Type	Event Code**	Driver ID	Moving Not Mvg	Date-Time Group	Odometer Reading	Latitude at Event***	Longitude at Event***	Place or SBC Code***
Nomenclature	Duty Status Change = D St Border Xing = B Last Record is Error = E Driver Compliance Review = R Records Inspected = I	On Duty=D, Off Duty=O On Duty, Not Driving=N Rest (Sleeper Berth)=R	Driver=D Co-Driver=C	Moving=M Not Moving=N	Value is number of seconds from a predefined date-time	Value passed directly from ECM with no encoding	Up to 8 digits stored as Long Integer with last 6 as fraction	Up to 8 digits stored as Long Integer with last 6 as fraction	Up to 7 digits stored as Long Integer

* US denotes unsigned which is what is used under SAE J1587 for this message

** Blank if Event Type does not equal D

*** Blank if Event Type equals E

Table 4 – Notional 24 byte record

There will be some number of events recorded during a trip, each one using 24 bytes of storage in the media used by the “front-end” solutions. This combined with the space taken by the pre-loaded data and the dedicated storage for the embedded key information in the card total to the storage used for the entire trip. These limits will almost certainly not be a problem in PDA or PocketPC CPU solutions as they enjoy 4 megabytes (MB) of storage or more.

The total amount used is much more critical for smaller passive (no internal power supply) media like SmartCard (SC) and Contact Memory Button (CMB) devices. The next section addresses media limitation based on the aggregate dataset that would be accumulated for a trip.



3.4 Media Limitations

The media that might be used in HOS solutions need to have enough capacity to contain a trip's worth of HOS data. Assuming 20 KB of space required for the pre-loaded information and 1,500 24 bytes records as being sufficient for a trip's worth of data implies $20,000 + (1,500 * 24)$ or 56,000 bytes of capacity. This is assumed as a minimum requirement

3.4.1 Portable Media

In general portable media allows the storage of information directly with some offerings incorporating independent cryptographic processing capabilities. The devices described here usually have very small form factors and do not have intrinsic power supplies but rather employ persistent circuitry that maintains the stored information indefinitely. Applications for HOS solutions would range from very small CMBs about the size of a dime to SC that usually emulates a Credit Card-sized form factor.

The next three sections provide a brief description of portable media directly applicable to HOS solutions.

3.4.1.1 Contact Memory Buttons

Contact Memory Buttons are passive devices that can read and write data when brought into physical contact with specialized hardware. This hardware can in-turn interface directly with computers as a peripheral device, which in this case would provide the interface to a "font-end" or "back-end" HOS solution. The primary advantage of memory buttons is durability as these devices are self-contained in a corrosion resistant case. They can handle from just a few thousand bytes to upwards of 350,000 bytes which is sufficient for a HOS Solution.

New and upcoming devices from Dallas Semiconductor have a built-in Java Virtual Machine (JVM) that can perform the free-streaming encryption needed to secure the HOS data, freeing the CPU from this processing load. More importantly, these chips are now available with a perpetually running real-time clock that could provide highly accurate and virtually tamperproof date-time groups to the records as they accumulate. Unlike the SmartCard these CMBs could be re-used as the encryption mechanism is self-contained whose key data would not be permanently "burned" into the card.

Their largest disadvantage is the physically small size (from the size of dimes to quarters) and relatively high cost (as compared to SmartCards) with the JVM and clock options but could be a part of HOS solutions.

3.4.1.2 SmartCards

SmartCards utilize an embedded chip that is usually mounted on a credit card form factor, allowing the card to be inserted into a slot form factor device that reads and/or writes data. Current SmartCard manufacturers typically provide cards with security features but not the clock option. They are available in capacities well above the HOS requirements. Most manufacturers have 64KB products that would fit nicely into the HOS estimated capacity requirements.



Hours of Service (HOS) Data Record Structure and Data Security

The credit card form factor and reasonable durability are a good fit for the HOS solutions. In bulk quantities the price will average about \$7-\$9 a card.

3.4.1.3 Flash Memory

Flash memory is currently available in a wide variety of form factors with current capacities approaching 1+ GB, thousands of times more than is required for HOS. Flash memory modules and their attendant built-in security features, would be the natural choice for PDA-centric solutions. With their capacity the entire HOS software and partitioned storage could be held in the Flash Card which would maximize security. The data pre-load and eventual recovery could be done with 'Back-end' solution specialized hardware. While in the vehicle the flash card would be held in the device whose CPU would articulate the reading and writing of the secured data.

3.4.2 Fixed Media

In general fixed media allows the storage of information directly; any cryptographic processing is handled by the software that is reading and writing the information. The two areas covered in the following sections depict the most commonly used storage in computers today. The section on Random Access Memory (RAM) will be present in almost any HOS solution as the Central Processing Unit (CPU) that performs the computations will need a place to store information.

The Magnetic Media section only applies to the various devices that would form the "back-end" portion of the solution and encompasses cartridge type, tapes, and the commonly used Hard Disk Drives (HDD) that form the backbone of data storage in computers.

3.4.2.1 Random Access Memory

PC's generally have two modes of storing information as they operate; the so-called High Speed and Low Speed storage modes. High speed storage uses Integrated Circuit (IC) technology allowing the information to be read and written very rapidly. The IC RAM chips have an average access time (time to get the pipe opened to the location at which the information will be stored) usually between 10 and 50 nanoseconds (Billionths of a second) with the rate of transfer dependent on the data bus of the device, usually between 60 and 120 megahertz (MHz or millions of times a second).

The memory comes in two types, persistent and non-persistent. This means that the memory chip either retains the information once stored or loses it when the computer is shut down. Non-persistent RAM is most commonly found in PC's and does not retain the information when the machine is shut down. This memory is generally less expensive and PC's almost always have magnetic-based storage in the form of HDD's that hold the information when the machine is shut down. Persistent RAM usually has much less capacity and is commonly found in devices that use firmware computing to operate but need to keep information available all the time. Examples of this are calculators, digital telephones, microwave ovens, etc. HOS solutions that would use persistent RAM are primarily PDA's that need lots of storage (current between 4 and 32 MB) but whose small form factor precludes the use of a HDD to keep the information when powered down.



Hours of Service (HOS) Data Record Structure and Data Security

High speed storage can read or write 100's of millions of bits per second – much more than is required for HOS given the frequency and amount of data in the notional record presented earlier. The result is that any of the simple firmware or software solutions that use either type of RAM memory will be more than adequate.

3.4.2.2 Magnetic Media

This section addresses fixed magnetic media and the three types of devices that may be used in HOS solutions. They all use the same data transfer notion which is that a surface with a magnetically sensitive coating has 0 or 1 states analogous to the bit discussed earlier spread around on it. A read/write head moves across the surface and performs the state change very rapidly, allowing the data to be transferred as desired. The three classes of devices that are applicable to HOS are tapes, flexible, and platen devices.

Tape devices would be used in HOS solutions for backing up data and are usually small cartridges that are inserted into a peripheral tape drive unit. Batch software running scripts periodically back up the information for the system, in this case a “back-end” solution. There are dozens of tape form factors and peripheral mechanisms available and can store from a few 100 MB to 100's of GB of information – again well within the expected size of even the largest HOS implementation in a large carrier.

The biggest disadvantage of the tape systems is that they are serial devices; the tape has to be fast forwarded or rewound to get at a discrete piece of information. This is the primary reason that these devices are used for batch backups which stream the data to and from the tape in bulk, exploiting the serial nature of these devices.

Flexible magnetic cartridge systems also exist in many form factors. The most common example is the well known “floppy” disk which is a disc of Mylar with the magnetically sensitive coating on both sides. The disk spins and a read/write head moves along a radial path which allows discrete points on either surface of the disk to be accessed for data manipulation. A double sided floppy disk, on a PC, will store just over 1.4 MB of information.

Other form factors for these devices include the Zip drive, SuperDisk, and others that store about 100 times as much information in the same size. These disks use a stiffer substrate for the coating, making them mechanically stable at higher rotational speeds so they can store more data faster.

Any of the flexible magnetic media could be used for the “back-end” HOS solutions although it is unlikely that 1.44 MB floppy disks would see much use because of their relatively small capacity. The biggest use will be for the 100-250 MB cartridge systems that would allow the accumulating data to be stored and the cartridge removed and physically locked up to further prevent tampering.



Hours of Service (HOS) Data Record Structure and Data Security

Platen disk drive systems are the third class of these devices and would only be used in the “back-end” systems. These represent the numerous form factors for HDD’s that virtually all PC’s utilize. They are like flexible media but the substrate is a rigid (usually aluminum) disk (the “hard” in hard disk) that allows much higher rotational speeds (systems are now approaching 20,000 RPM’s) and multiple platens with the read/write heads sandwiched in-between.

Storage capacity in these devices runs from about 100MB up to 250GB for a PC-sized single device. There are also concepts for forming arrays of these disks with failure recovery (the so-call Redundant Array of Independent Disks (RAID) that form much higher capacities in the 100’s of TB’s of storage. Even the smaller sized drives would handle HOS solutions efficiently as the small data record, designed to minimize cost and complexity in the “font-end” system pays off by not encumbering the “back-end” system’s storage capacity.



SECTION 4 – DATA SECURITY

4.1 Data Security Basics

Data security in general is enabled by the field of Cryptography. For most automated systems, of which HOS is a good example, the need to secure stored data and is concerned with keeping communications private.

The industry definition is that “encryption is the transformation of data into a form that is as close to impossible as possible to read without a unique string of characters that provides a key (or keys) for locking and unlocking the data”. The key(s) ensure privacy by keeping information hidden from anyone without the key(s), especially those who have access to the encrypted data, shouldn’t have, and are trying to decrypt it. Decryption is the reverse of encryption - the transformation of encrypted data (called ciphertext) back into a readable form.

The automated systems that perform these operations are generally referred to as cryptosystems which is a term used frequently in data security literature. Later sections will briefly describe their breadth and which ones are applicable to the HOS problem. The three main data security terms which have applicability to the HOS problem are briefly described below.

First, the data must be *trusted* as it passes from the initial preload of HOS data to the end where the trips-worth of HOS records are processed and stored on a “back-end” solution. Organizing who has encryption and/or decryption rights and what procedures are used in manipulating the data end-to-end should be structured to minimize tampering at the carrier level.

Secondly, depending on who pre-loads the data and who recovers it, the encrypted data winds up being recovered by someone not known to the originator. To be able to audit who has had control of the data from start to end the originator and ultimate receiver of the data should be *authenticated* to one another. This data, stored in the archival copy of the HOS data would allow the best possible re-construction of who, what, where, and how the data was originally accumulated for audit and inspection purposes.

Lastly, the HOS data that is gathered and stored must be *secure*. Encrypting the data makes it very difficult for the driver or an “on the road” 3rd party to tamper with the data. Several algorithms have been developed that form the mathematical engine, enabled on the computer by software, that does the encrypting and decrypting of the data. They use uniquely constructed strings of characters (the so-called key(s)) to move the data back and forth between the encrypted and decrypted states.

The next three sections cover the Trusted, Authenticated, and Secured aspects of the data security for HOS solutions.



4.2 Trusted Data

There are two basic methods of cryptography applicable to HOS that bear mentioning at this point. They are covered in the next two sections.

4.2.1 Secret-Key Cryptography

Symmetric or **secret-key cryptography is the traditional method**. . The assumption here is that some amount of data needs to be encrypted and sent from one person to another. Both the sender and receiver have a single secret key that enables either one to encrypt or decrypt the data, allowing them to exchange information. The data is only as secure as the key and ciphertext is kept from others that want to decrypt and read the data.

The HOS situation is similar. It is assumed that the sender is the person that pre-loads the data and implants the key (or keys) in the media such that the receiver, the person that recovers the HOS data at the end of the trip, decrypts it to assess whether the trip met HOS standards. In between these two persons is the driver(s) periodically adding HOS records to the media, using the key implanted in the HOS media, to secure the trip events. The intent is to deny the driver(s) **any** access rights to the data so tampering cannot take place directly. This leaves the driver(s) with only indirect methods for tampering (altering the time in the ECM, etc.) the intent could be captured by analyzing the HOS records in aggregate at the end of the trip.

4.2.2 Public-Key Cryptography

The second method is to employ the newer **public-key cryptography** which is designed to allow connections between sender and receiver who have a reason to exchange encrypted data but do not know each other (for example when you buy something on-line). Each person gets a pair of keys, one called the public key and the other called the private key. The public key is published, while the private key is kept secret. The need for the sender and receiver to share secret information is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. In this system, it is no longer necessary to trust means of communications, in this case the trip and associated HOS records.

The only requirement is that public keys be associated with their users in a trusted manner so the person with no knowledge of the other can get the correct public key. Anyone can send a confidential message by just using public information (the public key would be on the HOS media), but the message can only be decrypted with a private key, which is in the sole possession of the intended recipient, in this case the HOS data receiver at the end of the trip.

The primary advantage of public-key cryptography is increased security and convenience: private keys never need to be transmitted or revealed to anyone. Another major advantage of public-key systems is that they can provide digital signatures that cannot be repudiated, helping with Authentication (see next section).



4.2.3 Digital Envelopes

It is recommended a hybrid approach with public-key cryptography used in concert with secret-key cryptography to get the best of both worlds. This exploits the security advantages of public-key systems and the speed advantages of secret-key systems. This is commonly called digital envelope cryptography.

Secret-key systems require users to agree on a unique key to be used for some amount of data exchange, in HOS a trip during which the records are accumulated. The digital envelope consists of messages encrypted using secret-key cryptography which will perform well in simpler firmware HOS solutions with an encrypted secret key. The increase in performance comes from using a secret-key cryptosystem to encrypt the large and variably sized amount of message data, reserving public-key cryptography for encryption of short-length keys.

The digital envelope notion is also extensible to eMail systems where the single sender can enable multiple receivers of the information at different levels. For HOS, this could be exploited in large organizations where the HOS data may need to be inspected by multiple receivers of the information. Assuring that the data remains trusted through all of this is dependent on effective Key Management, which is discussed in the next section.

4.2.4 Key Management

Key management deals with the secure generation, distribution, and storage of keys. Once a key is randomly generated, it must remain secret to be effective. In practice, most attacks on public-key cryptosystems usually focus on the key management portion, rather than at the cryptographic algorithm itself. It's easier to get the key data and use it until discovered than it is to crack the encryption to read the data. HOS solution users in a large carrier organization must be able to securely obtain a key to keep HOS records trusted.

There are many schemes for key management and by far the most used and is called Public Key Infrastructure (PKI) which we would recommend for sending data within large carriers after recovery. This will offer the best overall solution for the HOS data once it has been received and should give the best tamper resistance to the data in the "back-end" systems.

For the media itself the schemas currently used in SmartCards, and there are many, would offer sufficient security to defeat the driver instigated tampering.

The situation is somewhat different for small operators where, in many cases, the pre-loader, driver, receiver, and archivist of the HOS data are all the same person. The best bet in this case is to have the HOS solution use PKI and the web to keep the data encrypted end-to-end with the rights extended to the user to only read but not manipulate the data.

4.2.5 The Escrowed Encryption Standard

There is another aspect of Key Management that bears mention as well. FIPS 194 – Escrowed Encryption Standard (EES), published in February 1994, was put in place to allow encrypted information to be decrypted by "lawfully authorized" officials. Its purpose is to allow law enforcement agencies the ability to access encrypted information during investigations to uncover criminal activities.



Hours of Service (HOS) Data Record Structure and Data Security

EES is also applicable to HOS. Investigators need access to driver's HOS records in progress. Accordingly, drivers also need to be able to review their records during trips, and like the inspector as has to carry the key(s) with the data.

It is important to note that the inspector and driver need only be able to read the records, applying computations to assess that the HOS are valid or not. To implement EES the Key Management system mentioned in the last section is modified into what is called a key escrow encryption system which is an encryption system with a backup decryption capability that allows authorized persons (users, officers of an organization, and government officials), under certain prescribed conditions, to decrypt ciphertext with the help of information supplied by one or more (usually two) trusted parties who hold special data recovery keys.

The data recovery keys are not normally the same as those used to encrypt and decrypt the data, but rather provide a means of determining the original data keys used to scramble the data in the first place. The key escrow notion refers to safeguarding the data recovery keys.

There are two or more parties that hold pieces of the data recovery key and that the requesting official must authenticate themselves to those parties under the correct conditions to move forward with getting at the data. All of this implies easy communications between the requester and escrow agents which would certainly be easier in audits performed on the accumulated records stored in a back-end system but more difficult in field inspection.

Much of the EES development recently has centered on near real-time interception of both telecommunications vice and data (encrypted phone conversations) as well as covert recovery of stored data (primarily for financial records) neither of which probably directly applies to HOS.

Unless the Government desires to be able to covertly access a Carriers records much of the EES technology will probably not be required. The driver will have the ability to review his records with a function that recovers the encrypted data and computes his compliance to the HOS rules. This analysis recommends that another event be added to the HOS data record that indicates when a driver reviews his own HOS compliance.

The inspector will need to review a driver's HOS compliance on an as-needed basis. In this case the escrowed system will not be very efficient and we recommend that the inspector physically view the driver as he is calling up a self-compliance check. After the inspection yet another event should be logged that indicates an Inspection was the reason for the HOS compliance to be reviewed. It is also recommended that a copy of the encrypted data be copied to the Inspector's machine to handle any downstream review and/or legal requirements.



Hours of Service (HOS) Data Record Structure and Data Security

It is recommended to keep data encrypted at all stages. Data would be encrypted during the trip continued when the data is stored afterward. The recommendation here is to maintain HOS records in a secure environment, with only authenticated users having the ability to read the data and compute HOS compliance.

It is also recommended that any authenticated user accessing an HOS record has the event logged both into the record itself (a log, encrypted like the rest of the data, would be appended to the HOS trip record) as well as an encrypted log in the “back-end” system storing the HOS record access activities. This will form a complete secure HOS record audit trail providing an effective deterrent similar to the EES component in the “back-end” system.

4.3 Authenticated Data

The PKI notions discussed above extend to the notion of a transparent (to the user) means of authenticating that who is accessing secure data. The broadly used term for this is Digital Signature and the governing document is FIPS 186-2(Change 1) which is effective as of July 2000.

Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory (the primary use for HOS record-keeping). In addition, the recipient of signed data can use a digital signature in proving to a third party that the signature was in fact generated by the signatory (which could be important for inspectors and auditors reviewing HOS records for a carrier that out-sources the HOS record-keeping. This is known as non-repudiation since the signatory cannot, at a later time, repudiate the signature.

A mathematical function is used in the signature generation process to obtain a condensed version of the data, called a message digest. It is used to produce a checksum, called a hash value or message digest, for a potentially long string or message. The message digest is then input to the digital signature algorithm to generate the digital signature. The digital signature is sent to the intended verifier along with any signed data. The verifier of the message and signature is verified by using the sender's public key. The same hash function must also be used in the verification process. The hash function is specified in a separate standard, the Secure Hash Standard, which is detailed in FIPS 180-1 – Secure Hash Standard (SHS).

By providing secure authentication records indicating who, when, and why HOS records were read forms an end-to-end audit trail for the data. This will serve as an additional deterrent against tampering as there is a risk to the person who tampered as being directly identified. As in any data security system the viability of the data is only as good the private keys are kept secret.

This analysis recommends that the usual security precautions be required for the “back-end” systems for direct access via user ID's and passwords. This includes more complex procedures such as requiring password changes at some frequency as well as some formal vetting of the carrier staff that will have widespread access rights.



Hours of Service (HOS) Data Record Structure and Data Security

Since the data need only be kept for six months it also recommended that the data is moved to a durable read-only media as soon as possible. The commonly used Compact Disc- Read Only Memory (CD-ROM) is the easiest and best to use. CD-ROMS are durable and cannot be written to once the data is recorded on the disc. It is impossible to directly tamper with the data once it's on the CD-ROM.

The data is secure and the disc is portable and can be physically secured as well. Furthermore, in the event of an audit of a carrier, the entire suite of records for the six-month period could probably be copied onto 1 or a few CD-ROM(s) for audit review. The peripheral hardware is inexpensive with 700 MB of storage for about 25 cents.

4.4 Secure Data

Most cryptographic systems are designed around securing much larger volumes of data than HOS will require. The typical encryption levels that secure on-line transactions and electronic funds transfers should be adequate for HOS purposes.

4.4.1 The Data Encryption Standard (DES)

Until early this year, the Data Encryption Standard (DES) mandated by FIPS 46-3 in 1977 on an algorithm initially developed by IBM for securing financial and military data, has been the de-facto standard. As computers (and the ability to break the encryption) has naturally progressed the DES standard has been modified three times (the -3 in the FIPS number) with the latest version, formalized in October 1999, called Triple DES (3DES), which is based on the ANSI X9.52 Triple Data Encryption Algorithm (TDEA, both the terms 3DES and TDEA frequently appear in the literature and can be used interchangeably). TDEA does not change the underlying DES mathematics but uses 3 keys, called a key bundle (the Triple in Triple DES) and a much different way of using them as the data is encrypted to make the ciphertext much harder to break as in the original 1977 version.

FIPS 46-3 allows either DES or TDEA to be used but states that "new procurements to support legacy systems should, where feasible, use Triple DES products running in the single DES configuration." – Single DES is a mode of operation in TDEA. These modes of operation tailor the mathematical encryption engine for different functional situations. There are 4 modes for DES (explained in detail in FIPS 81 – DES Modes of Operation) and 7 for TDEA (explained in detail in ANSI X9.52 – Triple Data Encryption Algorithm Modes of Operation).

These various modes of operation allow varying levels of data security and are tailored for batch data, free-streaming data, and other modes of operation. The HOS data is simpler to handle as the accumulating data has two modes. The first is the 20KB represents the pre-loaded data, securely stored at the beginning of the trip. After that is in place the remainder of the data are the infrequently placed 24-bit records which lend themselves to the block cipher mode of operation. Block Cipher encryption simply means that the data to be scrambled is sliced up into fixed length blocks, each one encrypted by applying the key(s) to the cryptosystem's algorithm, and then stored as equivalent blocks of ciphertext.



4.4.2 The Advanced Encryption Standard (AES)

As the Internet and electronic Commerce (eCommerce) proliferated the computing and telecommunications world a more flexible encryption system was needed. Between 1995 and November 2001 the Advanced Encryption Standard (AES) has come into being through FIPS 187. The standard became effective on May 26, 2002 and is based on an a Symmetric Block Cipher Algorithm (SBCA) that uses 128 bit blocks using keys of 128, 192, or 256 bits. Symmetric means that the same key(s) are used to encrypt and decrypt the information.

The winning AES algorithm is the so-called Rijndael Block Cipher and would be an excellent choice to handle the data security needs of HOS both being new and tailored for PC level processors as well as currently mandated for Government IT systems. TDEA running in the DES mode would also be acceptable as well, it looks for blocks of information.

4.4.3 HOS Applicability

Either 3DES or AES could be used with the 24-bit notional record described earlier. Given the time until an HOS regulation would require a specific algorithm, the AES is probably the most appropriate as it is more optimized for PC computing and will have further subsumed 3DES in the intervening time.

AES uses a 128-bit (or 128/8 which is 16 bytes) block cipher. The two 16 byte blocks (32 total) could be used to encompass the 24 byte notional record discussed earlier with 8 bytes for expansion. The encryption would only have to handle 2 block encipherments for each HOS event which would ease the computing burden on the less complex firmware solutions.

4.5 Relevant U.S. Government Standards

The Federal Information Processing Standards (FIPS) is a long-standing and evolving suite of documents that spells out the mandated (for federally developed systems) standards for a broad range of IT subjects. For data security there are 16 FIPS documents that bear on HOS solutions, some of which have been mentioned in the preceding sections.

Some of these standards apply solely to the “back-end” systems that would be used in large organizations where the IT users and administrators may not know each other personally. In these situations there are more generalized procedures for securing the data that may not be necessary in smaller organizations where the “power” users with secure data permissions all know each other and do not need additional physical and logical security measures.



Hours of Service (HOS) Data Record Structure and Data Security

Table 5, shown below, lists the 16 FIPS documents and their basic relevance to HOS solutions employing secured data.

FIPS	Title	Acronym	Relevance
31	Guidelines for Automatic Data Processing Physical Security and Risk Management		General Practice for setting up and maintaining secure computing facilities ("back-end" at carrier)
46-3	Data Encryption Standard (DES)	DES	The just subsumed secure algorithm, change 3 is Triple DES which is the current standard
73	Guidelines for Security of Computer Applications		General Practice for the design and development of computer programs with encryption routines
74	Guidelines for Implementing and Using the NBS Data Encryption Standard		Original Guide for configuring and using cryptosystems - referenced in other, newer standards
81	DES Modes of Operation		Illustrates the 4 DES Modes of Operation
87	Guidelines for ADP Contingency Planning		Guidelines for Contingencies. Describes practices for Disaster Recovery and day-to-day operations
112	Password Usage		Guidelines for vending and maintaining user passwords
113	Computer Data Authentication		
140-2	Security Requirements for Cryptographic Modules		Guidelines for protecting software and associated data in cryptosystems
180-1	Secure Hash Standard (SHS)	SHS	The hash standard used in PKI Authentication
181	Automated Password Generation (APG)	APG	Guide for vending computer generated passwords, used for large user communities in large carriers
185	Escrowed Encryption Standard (EES)	EES	The Official (and controversial) Escrow Standard
186-2	Digital Signature Standard (DSS)	DSS	The Standard for Digital Signatures that would be used for identifying HOS users for audit purposes
196	Entity Authentication Using Public Key Cryptography		The Guidelines for using PKI-enabled Authentication, used to establish an end-to-end audit trail
197	Advanced Encryption Standard (AES)	AES	The new algorithm - recommended for HOS
198a	The Keyed-Hash Message Authentication Code (HMAC)	HMAC	Hash standard for machine-to-machine authentication, could be used in large "back-end" systems in large carriers

Table 5 – Applicable FIPS Standards

The five rows in the table that are **bolded** indicate FIPS standards of special interest for HOS data security. The next five sections describe the relevant portions of these documents with respect to the HOS solutions.

4.5.1 FIPS 46-3 – Data Encryption Standard

FIPS 46 is the original data security standard and its based on an algorithm IBM developed in the 1970's and then gave unlimited rights to the Government for its use in it's IT systems. As time progressed DES has been modified for more security and currently in mandated as Triple DES (3DES) which uses the same underlying algorithm but serially applied three times with different keys for added security



Hours of Service (HOS) Data Record Structure and Data Security

A DES key is 64-bits (8 characters) long of which 56 (7 characters) are randomly generated – the remaining 8 are used for parity error checking and do not effect the encryption of the data. Note that the active 56-bit portion of the key is randomly generated and therefore incomprehensible as readable text. The random number generator used, and especially how its routines are created are all part of the Key Management discipline described earlier.

The data that will be encrypted is also posed in 64 bit (or 8 character) blocks, which would work well with the notional 24 byte HOS record which would be exactly 3 DES block encipherments. Deciphering is accomplished by using the same key that was used to encipher, but with the schedule of addressing the key bits is altered to guarantee that the deciphering process yields the original data.

The DES encryption process takes the block to be enciphered and subjects it to a mathematical permutation (called the Initial Permutation (IP), then a complex key-dependent computation is performed, and then a final mathematical permutation which is the inverse of the initial one (called the IP^{-1} permutation).

The complex translation done in the second step is defined in terms of two functions: the first is the f function (called the cipher function) with the second one employing the key(s) in the so-called key schedule (KS) function. The bulk of the rest of FIPS 46-3 plows through the math in excruciating detail, showing the extensions to the 3DES standard currently mandated.

DES could be used but the new AES standard will probably be in place and supported more directly by the time a mandated HOS regulation requiring formal data security is in place. The next section covers the Escrow Encryption Standard that was formalized in February 1994 to allow officials to covertly recover and decrypt secure data.

4.5.2 FIPS 185 – Escrowed Encryption Standard

The EES Standard described in FIPS 185 is primarily concerned with allowing the near real-time interception of encrypted voice and data over phone lines – this includes data transmitted via modems – which could be used in the “back-end” portion of HOS as well as some “front-end” solutions employing cellular phone technology.

The bulk of the document covers the basics of the SKIPJACK and LEAF protocols that are the methods used to access the data. There is discussion of the notion of escrow agents and their roles in re-constituting the key(s) needed for an official to access data. There are two or more parties that hold pieces of the data recovery key(s) and that the requesting official must authenticate themselves to those parties under the correct conditions (which are only described as “lawful authorized” in the document) to access the data.

The two algorithms themselves are classified and maintained by the National Security Agency (NSA) and are of course not discussed in detail. Under many conditions the algorithms are firmware in that dedicated chips are employed – this is necessary primarily in streamed data where real-time encryption is required.



For HOS solutions the escrow notion loosely applies to both the inspector in the field as well as carriers that would naturally accumulate HOS secure data over time. The driver will have the ability to review his records with a function that recovers the encrypted data, computes his compliance to the HOS rules, and informs him of the results. The inspector could use the same function, physically viewing the results which would allow a simpler field inspector system for field inspections to only need to get a copy of the encrypted data for downstream legal actions if a citation is issued.

For the carrier the escrow system could also be employed and whether it should or not depends on whether the Government desires to be able to covertly access a motor carrier's records directly. If not then the EES technology in general would not be required. The next section talks to the digital signature and PKI notions to assure Authenticated users are getting at the data.

4.5.3 FIPS 186-2 – Digital Signature Standard

In large systems there are frequently individuals exchanging secured data that do not know each other. Audits are also used to track who has had access to secure data and the notion of Authentication was formalized in FIPS 186 which is now at Rev 2, Change 1 as of January 2000.

The document describes three methods, all promulgated by commercial companies that can accomplish digital signatures. They are:

- (1) The Digital Signature Algorithm (DSA) is the Governments DSS of choice. It uses secure hash code (as defined by FIPS 180-1) to perform the DSS functions in the context of PKI, using both public and private keys to authenticate the individual as needed. The Private Key forms the digital signature and the public key authenticates it.
- (2) FIPS 186-2 also recognizes the RSA Labs (RSA stands for Rivest, Shamir and Adleman, the founders of RSA Security, Inc.) which was formally adopted in ANSI X9.31. It also uses a form of PKI and has been included mainly because of its excellent performance and widespread use.
- (3) There is also the Elliptic Curve Digital Signature Algorithm (ECDSA) that is an analog to DSA. It was adopted with ANSI X9.62 and also uses PKI.

The bulk of this document covers the precise mathematics for DSA and provides references to the ANSI standards for the other two.

Any of these could be used in HOS solutions. This analysis recommends that some form of authentication be used in the “back-end” solutions so an end-to-end audit trail is kept with each trip-specific archival record as well as a master audit log (in a secure database) that shows all users that have accessed the records. This master log may also act as a deterrent to tampering as the log would probably only be accessible by a few individuals in a large organization.

4.5.4 FIPS 196 - Entity Authentication Using Public Key Cryptography

FIPS 196 was issued in February 1997 to specify how the PKI notion was used to assure authentication via digital signatures. It specifies two challenge-response protocols by which



Hours of Service (HOS) Data Record Structure and Data Security

entities (users or computers exchanging data between them) can authenticate themselves. The authentication can be used at any time the “entities” are connected. Depending on which protocol is implemented, either one or both entities involved may be authenticated. The two protocols and the relevance to HOS solutions are:

- (1) The Unilateral Authentication Protocol (UAP) or so-called “Two-Pass” authentication is used where the requestor of the information authenticates the entity that provides it but in turn does not authenticate them self to that providing entity.
- (2) The Mutual Authentication Protocol (MAP) is similar but completes the loop where the entities involved are authenticated to each other before the information is passed from provider to requestor.

The MAP would probably be used for HOS “back-end” solutions as the Requester will be a human and the provider a computer (which needs to log the fact that the requester got the data for audit trail purposes). Using UAP would tell the requestor that they are getting the correct data but not provide his identity to the providing computer for the logs.

The next section covers the successor to DES and 3DES which has been mandated for new development since May of 2002.

4.5.5 FIPS 197 – Advanced Encryption Standard

FIPS 197 documents the new AES that is to be used in new developments. The AES employs a block cipher algorithm that processes 128 bits (16 characters) at a time, twice the size of the DES block. Furthermore the key(s) that are used can have varying length, depending on the strength of the encryption desired. The key lengths are 128, 192, or 256 bits (16, 24, or 32 characters).

A high-level description of how AES works centers on using the binary representations of each key’s character to form finite field elements a that are arrayed in prescribed fashions to encipher the data. The field elements are formed into a 2-D State Array that transforms the input.

This transformation is done using combinations of the modulo XOR addition and 8th order irreducible polynomial multiplication functions 10, 12, or 14 times (depending on the key length). At each step in the iteration the columns of the state array are mixed and the rows shifted in a prescribed pattern which results in a very strong encipherment. The process is reversed to decipher the data.

This a more flexible arrangement than DES and the algorithm performs better on PC’s as the mathematics, for the most part, operate at the byte level. This makes it the logical choice for HOS solutions.



SECTION 5 - RECOMMENDATIONS

The recommendations covered in the body of this document are compiled here in two sections, one for the Data Standard that could be used to compile the HOS data accumulated during a trip and the other to address Data Security to minimize intentional tampering by the driver(s) and/or carrier as well as guarantee the privacy of the data in general.

DATA STANDARD RECOMMENDATIONS

The most important recommendation is that **the same HOS Data Standard should be in all HOS solutions**. The FMCSA Regulation Section 395.15 encompasses 15 discrete datums that need to be gathered every time the driver status changes during a trip. Additionally the Government desires to capture the location when the vehicle crosses State borders. All data should be securely stored in a common format regardless of the HOS solution. The resulting simple format will maximize flexibility for the wide range of “front-end” HOS solutions that will emerge while lessening the burden for archival storage in the “back-end” solutions.

Furthermore, **the HOS Data Standard should utilize commonly accepted character and numeric encodings** for the characters that are stored in the record. Recommend the use of the UNICODE UTF-8 (same as the extended ASCII character set) that yields 1 character for every 1 byte of data for text and the standard PC-based signed long integer that stores values between -2,147,483,648 and +2,147,483,647 in 4 bytes of data for numbers.

Numeric codes should be used to designate the locations, using the standard long integer encoding. This will allow solutions with GPS receivers to provide the latitude and longitude of the driver status change or state border crossing for which the code will be looked up and then securely stored. For solutions with no GPS the software would re-use the same look up data to allow the driver to navigate a few menus with state, city, and/or road names at which point the code is extracted and securely stored.

The HOS data record should be as logically small as possible to facilitate firmware solutions (less storage capacity and computing power) and also data archival storage in “back-end” systems. Section 2.3.3 suggests a 24 byte long record that could contain all the data required for FMCSA Regulation Section 395.15, less the pre-loaded information which is securely stored before the trip begins by the carrier. This allows the widest range of storage media to be employed, from SmartCards in the “front-end” systems to high-capacity hard disk drives in the “back-end” systems.

The vehicle’s ECM should be used as the primary data source for Odometer and moving/not moving datums in the record. Initial examination of the J1708 and J1587 available messages indicates that both a primary and backup source from the ECM is available for these datums. The use of the ECM in general will be described in detail in the next report “Research and Analysis on ECM/TCM Usage for HOS Solutions”.



Hours of Service (HOS) Data Record Structure and Data Security

If a GPS system is available it should be used for the date-time datum in the record as this source is much more tamperproof. If a GPS system is not available then the ECM clock should be used for the date and time. Initial examination of the J1708 and J1587 available messages indicates that both a primary and backup source from the ECM is available for these data. The use of the ECM in general will be described in detail in the next report "Research and Analysis on ECM/TCM Usage for HOS Solutions".

Any HOS design specification should stress the need for an integrated GPS system. Having a GPS system available for the HOS solution to discretely demand the date-time and location almost completely automates the HOS data-gathering process and would provide the most tamper-resistant solutions.

DATA SECURITY RECOMMENDATIONS

HOS solutions should enforce trusted, authenticated, and secure data for maximum privacy and resistance to tampering.

Trusted Data Recommendations

The HOS data passes from the initial preload to the end of the trip where the records are processed and stored on a "back-end" solution; during this time the originator and driver(s) write the data and other read it via the "back-end" systems. Organizing who has encryption and/or decryption rights and what procedures are used in manipulating the data end-to-end is extremely important.

"Digital Envelopes", which uses both public- and private-key methods for encrypting the data for a trip, should be used to provide trusted HOS records. This will provide the best mix of a robust encryption while utilizing the convenience of the PKI infrastructure that allows individuals or computer not directly known to be "trusted" to encrypt or decrypt the HOS data.

HOS "back-end" solutions should be implemented using PKI infrastructure to effectively manage the keys that are used to encrypt and decrypt the data. The well-established PKI techniques will provide an easy to manage security setup for carriers and many COTS solutions are available that can be quickly integrated into the HOS "back-end" solutions.

The "front-end" solutions that compute HOS records should use compiled software and then free-stream encrypt all HOS data for storage. This results in the HOS data records always being secure without the driver(s) needing key(s) to use the "front-end" system. This is analogous to the way eCommerce works on the web where a user exchanges secure data, never having to worry about the management of the encryption key(s).



Hours of Service (HOS) Data Record Structure and Data Security

Data entry errors should be logged in the HOS record with the old and incorrect data retained for a full audit trail. This will provide anecdotal information for “back-end” systems that could process multiple trip records for patterns indicating attempted tampering.

The Government should consider less stringent data security requirements for individual operators. HOS solutions for small individual operations only need the ability to generate a key for encrypting the data without the need for the PKI infrastructure to facilitate communicating the secure data between individuals. This would limit direct tampering to the inputted data but still encrypt it end-to-end.

The Escrow Encryption Standard should not be used for HOS solutions unless covert access to carrier data is needed. Using the SKIPJACK and/or LEAF protocols will add significant expense to any “back-end HOS solution and this should not be implemented unless necessary.

HOS solutions should have a function that will safely inform the driver of his HOS compliance at any time. This function would access the accumulated records and compute the compliance based on the rules set by FMCSA Regulation Section 395.15. This will promote safety on the part of the drivers and also allow a less complex inspectors solution.

The inspectors system should have the ability to recover an electronic copy of the encrypted data but not be able to decrypt it. This will eliminate extending the carrier-specific PKI to inspectors but still allow them to get a copy of the encrypted data. Assuming the recommendation for keeping the data encrypted “end-to-end” is enforced; the inspector’s copy could be later compared to the final record to verify the portion up to the inspection was not changed.

Authenticated Data Recommendations

To assure that the HOS data is trusted it is important to authenticate the users that encrypt and decrypt it. This begins with the user at the carrier that preloads the HOS record (that identifies the driver(s)) and continues with the driver(s) that accumulate the HOS records, these are the only users that write to the data records.

After the trip is complete, the HOS compliance is verified, and the trip record is archived. Until the records are destroyed other users with access rights may decrypt and read the data, but not edit it. This assures the complete audit trail mentioned earlier with maximum tamper-resistance.

The Digital Signature Standard should be used to provide authentication and identification for all the authorized users that interact with the secure HOS data. Any of the 3 DSS algorithms are fully acceptable and any design specification should allow all three to minimize cost for the HOS solution developers. Using the different DSS algorithms is possible the carriers would control authentication internally, and the internal data security procedures would not encompass inspectors.

The PKI-based Authentication for audit logs should use the Mutual Authentication Protocol that identifies and authenticates both parties. This is required as the Requestor will



Hours of Service (HOS) Data Record Structure and Data Security

be a human and the provider a computer (which needs to log the fact that the requestor got the data for audit trail purposes).

The archived HOS records should have a secure log appended, with the originator, driver(s), and all the authorized users that read the HOS records until the records are destroyed. This will indicate when and who has accessed the data to provide the end-to-end audit trail mentioned earlier.

A master audit log should be established that holds HOS record access across the entire carrier organization. This will provide a cross-referenced source for data to articulate who has accessed multiple HOS records which should deter tampering. This also provides an index for “back-end” solution functions that could analyze and make reports about HOS compliance.

A Standard practice for access to the systems by authorized users should be implemented for large organizations. This encompasses things like a common password syntax, procedures for periodically changing login information, and many others. Carriers should consider a vetting process analogous to a background investigation for “power” users and those with administrative privileges on the systems to minimize the possibility of tampering or industrial espionage.

HOS records should be periodically stored on CD-ROM's (primary and backup with Disaster Recovery Procedures) and their storage in read/write media “hard” deleted (media physical locations bits set to zero). This will minimize downstream tampering that might be attempted to change a group of HOS trip records. As long as the CD-ROMS have good physical security they will be difficult to obtain, decrypt, copy, tamper with, encrypt, and replace in the “back-end” system.

Secured Data Recommendation

The currently accepted standards, DES and AES, are fully acceptable for the encryption of the HOS data.

The AES standard, mandated as of May 2002, should acceptable for HOS data encryption. Although relatively new, it is rapidly being enabled by COTS products and, by the time HOS automation will be mandatory, should be easy to integrate with the solutions.



BIBLIOGRAPHY

The 35 documents used in this research and analysis are listed below. Portable Document Format (PDF) files with this information in its entirety are included on the CD-ROM for this module.

#	Title
1	FIPS 31 - Guidelines for Automatic Data Processing Physical Security and Risk Management
2	FIPS 46-3 - Data Encryption Standard (DES)
3	FIPS 73 - Guidelines for Security of Computer Applications
4	FIPS 74 - Guidelines for Implementing and Using the NBS Data Encryption Standard
5	FIPS 81 - DES Modes of Operation
6	FIPS 87 - Guidelines for ADP Contingency Planning
7	FIPS 112 - Password Usage
8	FIPS 113 - Computer Data Authentication
9	FIPS 140-2 - Security Requirements for Cryptographic Modules
10	FIPS 180-1 - Secure Hash Standard (SHS)
11	FIPS 181 - Automated Password Generation (APG)
12	FIPS 185 - Escrowed Encryption Standard (EES)
13	FIPS 186-2-Ch1 - Digital Signature Standard
14	FIPS 196 - Entity Authentication Using Public Key Cryptography
15	FIPS 197 - Advanced Encryption Standard (AES)
16	FIPS 198a - The Keyed-Hash Message Authentication Code (HMAC)
17	FAQ About Today's Cryptography - RSA Labs
18	Public Key Infrastructure Primer
19	Network and Data Protection - A Security Primer
20	Cryptography Security and the Future
21	How to Evaluate Security Technology
22	Formalizing and Securing Relationships on Public Networks
23	Secure Audit Logs to Support Computer Forensics
24	Peer to Peer Software Metering
25	The Risks Of Key Recovery, Key Escrow, And Trusted Third-Party Encryption
26	A Taxonomy for Key Escrow Encryption Systems
27	Designing Encryption Algorithms for Optimal Software Speed on the Intel Pentium Processor
28	A Comparison of the 5 AES Finalists
29	The RijnDael Block Cipher for AES
30	Blowfish - A New Variable-Length Key, 64-Bit Block Cipher
31	Twofish - A 128-Bit Block Cipher
32	The Solitaire Algorithm
33	VB Data Type Summary
34	Dallas Semiconductor Java Secured CMB
35	Satellite Vehicle to Universal Coordinated Time Conversions in GPS



Federal Motor Carrier Safety Administration

Office of Business and Truck Standards and Operations

Research and Analysis on Engine Control Module and Transmission Control Module Usage for Hours of Service Solutions

January 21, 2003



ECM and TCM Usage for HOS Solutions

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
TABLE OF CONTENTS.....	II
SECTION 1 – EXECUTIVE SUMMARY.....	1
SECTION 2 - RELEVANT ECM SPECIFICATIONS.....	2
2.1 “Low-Speed” SAE J1708 and J1587 – Found in Many HD Vehicles.....	5
2.1.1 SAE J1708 - Serial Data Communications Between Microcomputer Systems In Heavy-Duty Vehicle Applications.....	5
2.1.2 SAE J1587 - Electronic Data Interchange Between Microcomputer Systems in Heavy-Duty Vehicle Applications.....	9
2.2 “High-Speed” SAE J1939 – Gaining Ground in HD Vehicles.....	17
2.2.1 J1939-11, J1939-21, and J1939-31 Physical Network Description.....	19
2.2.2 SAE J1939-71 – Vehicle Application Layer for Messages.....	20
SECTION 3 –ECM MESSAGE DETAILS FOR HOS SOLUTIONS.....	25
3.1 Demanding a Date-Time Group – Obtainable From Either Specification but J1939 More Tamper-resistant.....	26
3.1.1 J1587 or J1939-71 Date Messages.....	26
3.1.2 J1587 or J1939-71 Time Messages.....	27
3.1.3 J1587 Backup Date-Time Group via Elapsed Time Message – No backup in J1939-71.....	27
3.2 Moving/Not-Moving Related Messages – Numerous Alternatives.....	27
3.2.1 J1939-71 Drive Recognize – Direct Measure on “High-Speed” Networks.....	28
3.2.2 J1587 or J1939-71 Wheel-Based Road Speed – Primary M/NM Source.....	28
3.2.3 J1587 or J1939-71 Main Shaft Speed - Backup M/NM Source.....	29
3.3 Demanding the Odometer Reading.....	29
3.3.1 J1587 or J1939-71 for Total Vehicle Distance.....	29
3.4 Location-Related Messages for HOS Solutions on Vehicles with Integrated GPS Systems.....	30
3.4.1 J1587 and J1939-71 for Direct Location Data.....	30
3.4.2 J1587 for State Border Crossings – Only on “Low-Speed” Networks with Sophisticated GPS and On-Board Databases or External Communications.....	31
3.4.3 J1587 for Current State and Country– Only on “Low-Speed” Networks with Sophisticated GPS and On-Board Databases or External Communications.....	32
3.4.4 J1587 for Milepost ID – Only on “Low-Speed” Networks.....	32
3.5 J1787 and J1939 Messages to Augment and/or Check Pre-Loaded Data.....	32
3.5.1 J1587 or J1939-71 for the Truck VIN –Pre-Load or Tractor Swap Check.....	32
3.5.2 J1587 or J1939-71 for Driver IDs –Preloads Verification.....	33
3.5.3 J1939-71 for Driver Card– Could verify Preloads and Status Changes.....	33
3.6 J1939-71 Messages to Detect Clock Tampering.....	33



ECM and TCM Usage for HOS Solutions

3.6.1	J1939-71 Indicates a Changed Clock Parameter.....	34
3.7	J1939-71 Messages to Directly Recover Duty Status Changes	34
3.7.1	J1939-71 Bit States Showing Driver Status	34
SECTION 4 – RECOMMENDATIONS		35
BIBLIOGRAPHY		38



ECM and TCM Usage for HOS Solutions

SECTION 1 – EXECUTIVE SUMMARY

HOS solutions can greatly benefit from using data demanded discretely from Heavy Duty Vehicle Networks. Since the 1980's there have been dozens of standards developed across the automotive, trucking, and marine arenas to better control engines, transmissions, and other vehicle subsystems.

There are two standards, one well established and the other one relatively new, which can provide this data to any future automated solutions for recording HOS Compliance. Both specifications are promulgated by the Society of Automotive Engineers (SAE). The first and older specification is based on two documents, SAE J1708 for the networks physical and logical architecture and SAE J1587 for the messages that would provide the HOS data. The more recent SAE J1939 Standard provides the same information for the newer network type.

The older or "low-speed" J1708 standard runs at 9600 bits per second, the state-of-the-art when it was mandated while the newer "high-speed" J1939 standard runs at 250,000 bits per second – over 25 times faster. Both of these network types provide messages about Odometer and Moving/Not Moving data that could be used. Our research and analysis has yielded 13 "low-speed" and 26 "high-speed" messages that are applicable to HOS solutions.

These messages are all available on a discrete basis – the HOS solutions will send requests to the vehicle network with a response that contains the data returning. Some vehicles may not have the sensors and microprocessors installed to support all the messages called out in the document. If a particular message is not available both network types return a message indicating an error. The HOS solution Software Design Specification will need to define the minimum message support for HOS solutions as well as contingencies when message(s) are not available.

Table 12 on Page 25 of this document shows the mapping between the Part 395 data requirements and what "low-speed" and /or "high-speed" vehicle network messages address them. Of the 18 data items only 4 are not addressed by both network types. These 4 items would all be "pre-loaded" into future HOS records before the trip begins.

The older "low-speed" network offers less coverage for HOS compliance data but may be adequate for HOS solutions. The newer "high-speed" network offers more message data and is also fully adequate for HOS solutions.

Section 2 of this document describes the relevant ECM specifications providing lists of the 13 "low-speed" messages in Tables 8 and 9 on Pages 15 and 16, with the 26 "high-speed" messages listed in Tables 10 and 11 on Pages 22 and 23.

Section 3 lists the specific messages, ordered by individual HOS areas of interest (Duty Status Codes, determining time and data, etc.) with the applicable "low-speed" and "high-speed" message details portrayed.

Section 4 contains the recommendations, followed by a Bibliography listing the 45 documents used during the research.



SECTION 2 - RELEVANT ECM SPECIFICATIONS

Background

Engine Control Modules (ECMs) and Transmission Control Modules (TCMs) are devices that can be used to supply data for building HOS compliance records. From their inception in the late 1960's until the early 1990's, these devices and their attendant sensors have provided data about hundreds of vehicle functions.

The requirements for reduced emissions in vehicles in general spawned the use of Microprocessors to measure, compute, and then control the engine and drive train the road-going vehicles. Additional functionality was rapidly added to allow diagnostic information to be sensed and stored for later correction during maintenance. Initially much of this development happened in automobiles, rapidly followed in Medium- and Heavy-Duty trucks/buses – the class of vehicles under consideration for HOS solutions.

Early ECM's and TCM's were connected only to sensors physically near the controller. This meant that any diagnostic information stored in these individual devices made the downstream maintenance equipment more complex. As in any new (at the time) technology, the standards for the devices were not immediately mandated but more manufacturer-dependent.

The bulk of these were initially limited to the “big 3” automobile manufacturers and were:

1. General Motors (GM) used the Assembly Line Diagnostic Link (ALDL) also known as the 8192 Universal Asynchronous Receiver-Transmitter (UART) which is still in use. As implied in the ALDL acronym the device is used to assure that the vehicle is built-out correctly during manufacture, then benefiting from the device during operations.
2. Chrysler used the Serial Communications Interface (SCI) which is a 62.5 kbps standard developed by Motorola. This is also still in use with the same notional idea as the GM system and also provides a dedicated link between the ECM and any external test equipment.
3. Ford started with Audio Equipment in their Audio Control Bus (ACB) and Audio Control Protocol (ACP) which rapidly branched out to encompass engine control and other diagnostic functions with increased processing power and enhanced algorithms.

This answered the regulatory requirements requiring vehicles meet emissions standards but resulted in an industry without consistent standards. A number of State and Federal Government actions have moved the controlling devices in vehicles to be compliant with an “approved” list of communications standards. This umbrella standard is generally referred to as the On-Board Diagnostics II or OBD-II standard for vehicles and applies to automobiles and light trucks manufactured in Model Year 1996 and later.



ECM and TCM Usage for HOS Solutions

OBD-II requires a common Society of Automotive Engineers (SAE) J1962 connector that supports either the SAE J1850 Class B Communications Network Interface Standard for Vehicle Area Networks (VANs) or the ISO 9141 (commonly called the ISO 9141 CARB) standard. CARB is the California Air Resources Board which many times leads in emissions standards development.

J1850 was adopted by GM and Ford while Chrysler adopted the ISO 9141 standard for their automobile and light-truck products. Many foreign manufacturers also adopted the ISO 9141 as J1850 was being developed by the SAE. The common characteristics between the two network standards are the adoption of a physical (for hardware), data link protocol (to describe how – not what – data is moved around in the network), and finally an application layer for the data messages themselves.

Current Applicable ECM Standards

The standards described to this point do not apply to the Heavy-Duty vehicles that HOS solutions will need to interface, however they have evolved into three types – two of which bear directly on the HOS problem.

The first one is a standard found primarily in Europe and probably would not be a factor for HOS solutions. It is the Keyword Protocol 2000 (KWP2000) which is based on ISO 14230 with the physical layer re-used from the ISO 9141 standard mentioned earlier. Because the ISO 9141 is meant to physically model automobiles and light-trucks (essentially two axles, 2 to 4 tires, and no trailer) the use for HD vehicles is unlikely.

The other two HD vehicle standards are directly applicable to HOS and reflect two succeeding generations of technology in moving ECM's and TCM's into trucks and buses.

The first is the so-called "low-speed" standard which is defined by two SAE standards – one for the data protocol (how the data flows) and the other for the application layer (what the data contains). They are:

SAE J1708 - Serial Data Communications between Microcomputer Systems in Heavy-Duty Vehicle Applications – was issued in January 1986 and is still widely used today in HD vehicles as a networking solution. The data-bus is patterned on the RS-485 Serial specification and uses an unshielded twisted pair wire running at 9600 bits per second (bps). This low speed (by today's standard) was the state-of-the-art in 1986 and the RS-485 uses commands much like PC Modulator-Demodulators (MODEMs) to move the information around. This supports HOS solutions as the commands lend themselves to specifying a message and requesting data.



ECM and TCM Usage for HOS Solutions

SAE J1587 - Electronic Data Interchange Between Microcomputer Systems in Heavy-Duty Vehicle Applications – was also issued in January 1986 and is probably the most widely used system of diagnostic and control messaging today. The standard started out with 256 messages and was expanded during the 1990's with an additional 256 (there are currently 509 active messages in J1587) added to encompass the changing face of data requirements on HD vehicles.

This study identified 13 messages that are relevant to HOS solutions and could be used. The J1587 standard provides a list of all the possible messages that a truck could support, depending on it's specific equipment.

For example, there is a specific message for the truck location (State and County) but, to determine this as a datum the truck would have to have a GPS system and computer with a database that could take the GPS-provided Latitude and Longitude and compute the State and County. The average truck with an HOS solution installed will probably not have this luxury during HOS data gathering. Any software design specification should indicate that these messages should be polled with the solution falling back on other data gathering methods. This will result in HOS solutions that can be applied across the board – the software logic would adapt to the individual truck depending on it's equipment.

The second is the so-called “high-speed” standard which is defined by a single SAE standard that contains distinct documents for the data protocol (how the data flows) for the application layer (what the data contains). It is based in the Controlled Area Network (CAN) topology developed by Bosch in Europe which has been in continuous development since the late 1980's. The CAN standard has been development since the late 1980's and addresses data link and application layers as in the “low-speed” standard.

Version 2.0B was in place by the 1990's and with the aging “low-speed” standard for HD vehicles needing replacement saw the SAE J1939 standard come forward as the “high-speed” replacement. The entire specification is a single document which is the **SAE J1939 Truck and Bus Control and Communications Network Standards Manual**. There are stand-alone sections in the Manual that are analogous to the “low-speed” J1708 and J1587 standards which are:

J1939-11 Physical Layer, 250K Bits/sec, Shielded Twisted Pair (October 1999), J1939-21 CAN 29 bit Identifier Data Link Layer (July 1999), and J1939-31 Truck and Bus Network Layer document (December 1994). Taken together, they are analogous to the J1708 “low-speed” standard. J1939 “high-speed” networks are becoming more widely used in HD vehicles. The data-bus is patterned on peer-to-peer networking, the assumption being that many differing control modules and sensors all reside in nodes of the network.



ECM and TCM Usage for HOS Solutions

The controllers are able to communicate with each other as required. From this perspective the HOS solution would be another device on a node of the network, making the physical connection of the HOS solution much easier. Furthermore the network sustains about 250 kbps during operations; about 30 times faster than the “low-speed” standard for much better performance.

The J1939-71 Vehicle Application Layer Document (August 1994) is analogous to the J1587 “low-speed” standard is rapidly overtaking its “low-speed” counterpart in newly-constructed HD vehicles. The standard has over 2500 messages with many of the 509 J1587 messages re-used for compatibility in diagnostic equipment and procedures..

The greater number and type of messages in J1939-71 has yielded 26 messages that are relevant to HOS solutions and that should be utilized if the individual truck supports that message. As in the “low-speed” standard, the J1939 standard provides a list of all the possible messages that a truck could support.

Sections 2.1 and 2.2 cover the “low-speed” and “high-speed” standards respectively that are relevant to HOS solutions. They will provide more detail about the two standards and their applicability to HOS solutions. The messages that the HOS solutions would access are described in detail in Section 3 of this document.

2.1 “Low-Speed” SAE J1708 and J1587 – Found in Many HD Vehicles

The J1708 and J1587 “low-speed” standards were issued by SAE in January 1986, just at the time when computer technology was beginning to offer cost-effective components. At that point in time the fastest modems were communicating at 9600 bits per second and this was incorporated into J1708 coupled with a simple unshielded twisted pair physical wiring scheme. The whole thing is enabled by emulating the EIA RS-485 Standard for Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems (April 1983) which at the time yielded the best data throughput given the speed of the microprocessors involved.

The SAE J1587 defines the messages that can be articulated in the vehicle network. The “low-speed” standard uses a 2-tiered hierarchical system of Message Identification Numbers (MIDs) and Parameter Identification Numbers (PIDs) to uniquely identify a message. Any HOS solution would use these two numbers to demand the required data. This study has identified 13 message items applicable to HOS. At a minimum these messages will provide the date-time, elapsed distance, and moving-not moving parameters for most HD vehicles. Other messages could provide additional location and driver related data – assuming that the truck had devices that could report that data over the network.

2.1.1 SAE J1708 - Serial Data Communications Between Microcomputer Systems In Heavy-Duty Vehicle Applications

The J1708 specification defines a general-purpose serial data communication link for heavy-duty vehicle applications. The primary use of the protocol described in the standard provides a



ECM and TCM Usage for HOS Solutions

general-purpose communications link which is typically used to share data among stand-alone modules on a heavy-duty vehicle.

The J1708 standard describes the protocol that can be used to transmit and receive the data and not the character set or specific messages and their associated formats. As in most data transfer protocols the records are made up of characters consisting of 8 bits (1's and 0's) and the standard only mandates the length of a standard message (up to 21 characters). The first character is reserved for an unsigned 1-byte integer (allows a range of 0 to 255) that defines the Message Identification number (MID) for the message.

The MID specifies the area of the vehicle (engine, brakes, tires, etc.) that the rest of the message will concern. The only other parameter required by J1708 is a priority from 1 to 8 for the message (the smaller the number the higher the priority). The priority drives how quickly the message can be recovered by the ECM from an associated sensor or demanded from an external device (in our case an HOS solution). The information making up the message is provided by the J1587 standard described in section 2.1.2 of this document.

The J1708 standard communicates via a signal that contains Binary (1's or 0's) data and the unit time (also called the bit time) is prescribed at 104.17 msec. This yields a data rate in J1708 networks of 9600 bits per second (bps or baud) which was a "state of the art" speed at the time J1708 was mandated. This "low speed" (by today's standards) will limit the amount of data that can be moved and to some extent limit the access time that HOS data can be demanded as the messages that contain the data have varying priorities.

The next section describes the specifics of the overall data structure and the timing limitations for HOS solutions interfacing with the "low-speed" J1708 vehicle data networks.

2.1.1.1 Overall Data Structure and Timing Limitations

Central to understanding any limitations on HOS data demands is the time it takes to respond to a message. This is called Bus Access Time (T_a in Section 5.2.1.1 of J1708) and can vary significantly depending on a number of factors. All network topologies have to have a rigidly enforced frequency of operation and for J1708 networks this is based on an RS-485 spec at 9600 bits per second.

This means that 9600 ones and zeroes can be transmitted or received every second which implies that the period of time that one unit of information (a 0 or a 1) is $1/9600$ or about 104.17 milliseconds. This time unit is called the bit time (T_b in section 5.2.1.1 of J1708). The data that will eventually be placed in this stream will be made up of characters and numerical values encoded as numbers and each of these will use blocks of 8 bits, commonly called a byte of information.

J1708 is different than PC's in that the older modem-like operation it affects uses UART operations that add another bit at the start (the Low Level Logic Bit) and stop (the High Level Logic Bit) of the character for a total of 10 bits to a character in J1708 networks. This then implies that 9600 bits per second will yield $9600/10$ or 960 characters per second for "low-speed" HD vehicle networks.



ECM and TCM Usage for HOS Solutions

J1587 specifies a standard 21 character record structure or all messages which in turn implies 960/21 or at least 45 messages a second. To complicate things further the messages all have pre-assigned priorities which could delay the time it takes for an HOS demanded message to get a response. The worst case scenario is that an HOS solution demands a low-priority datum when the network is busy processing a series of high-level messages unrelated to HOS. This is most likely to occur when diagnostic limits are exceeded and data is being buffered for downstream maintenance.

In this case the driver of the truck would most likely be handling an engine or drive train problem and certainly not be inputting HOS Duty Status Changes. Priorities range from 1 to 8 and their nomenclature is depicted below in Table 1.

Priority	Message Assignment
1 and 2	Reserved for messages that require immediate access to the bus
3 and 4	Reserved for messages that require prompt access to the bus in order to prevent severe mechanical damage
5 and 6	Reserved for messages that directly affect the economical or efficient operation of the vehicle
7 and 8	All other messages not fitting into the previous priority categories should be assigned a priority 7 or 8Priority table

Table 1 – J1708 Message Priority Nomenclature

Contentions between competing microprocessors to send or receive a response to a message are First-In-First-Out (FIFO) with a higher priority bumping that message to the front of the list. The normal operation worst case access time can be computed with:

$$T_a = T_i + (2 * T_b) * P \text{ (Equation 1 from J1708, section 5.2.1.1)}$$

T_i is the expected idle time and can be as long as 19 High Level Logic Bits. Since these occur at the end of a character, 19 of these could take nineteen 10-bit characters or 190 bit times. So with T_i equal to 190 T_b and a Priority of 8 for a message the access time in seconds is $190/9600 + (2 * 1/9600) * 8$ or about .021 seconds which is a little less than 1/50th of a second. Even with 50 high priority messages stacked up in the FIFO buffer the message would be responded to within 1 second which will probably be acceptable for the HOS solutions

2.1.1.2 Message Identification Numbers

The first character of any “low-speed” message contains the MID. Since it is a character it consists of 8 bits and is interpreted using binary or Base 2 arithmetic. So the values for MID can range from 00000000₂ (in Base 2) which is 0₁₀ (in Base 10) to 11111111₂ or 255₁₀ making 256 possible values. The MIDs are broken out as in Table 2.

Message Range	Transmitter Category
00–07	<i>Engine – Moving/Not Moving and Clock Data</i>
08–09	Brakes, Tractor



ECM and TCM Usage for HOS Solutions

10-11	Brakes, Trailer
12-13	Tires, Tractor
14-15	Tires, Trailer
16-17	Suspension, Tractor
18-19	Suspension, Trailer
20-27	Transmission – Moving/Not Moving Data
28-29	Electrical Charging System
30-32	Electrical
33-35	Cargo Refrigeration/Heating
36-40	Instrument Cluster - Odometer
41-45	Driver Information Center – Multiple Data Items
46-47	Cab Climate Control
48-55	Diagnostic Systems
56-61	Trip Recorder – Location Data (if GPS Equipped)
62-63	Turbocharger
64-68	Off-Board Diagnostics
69-86	Set Aside For SAE J1922
87-110	Reserved—To Be Assigned By SAE Electronic Interface Subcommittee (See 6.3.2, Section 4)
111	Reserved—Factory Electronic Module Tester (Off Vehicle)
112-127	Unassigned—Available For Use
128-255	To Be Assigned By SAE Data Format Subcommittee

Table 2 – J1708 MID Ranges – HOS-related MIDs in *BOLD*

The MIDs in bold in the table above would contain the PIDs that uniquely identify possible HOS messages and are annotated. J1708 states that “MIDs in the range of 128 to 255 shall be reserved for applications using formatted data as set forth in a document issued by the SAE Truck and Bus Electrical Committee Data Format Subcommittee. These MIDs shall only be used when the data format set forth within that document is strictly followed. See SAE J1587.”

This means that all the HOS messages could also use MID’s specified in J1587 (section 2.1.2.1 of this document lists them). The next section briefly covers the RS-485 standard that drives much of the physical parameters of “low-speed” solutions.

2.1.1.3 Use of the EIA RS485 - Standard for Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems

RS-485 allows up to 32 microprocessors to communicate on a single unshielded twisted pair of wires at distances up to 4000 feet which is more than adequate for HOS solutions. Data is transmitted differentially on two wires twisted together resulting in high noise immunity. RS-485 networks can be configured two ways, “two-wire” or “four-wire.”

In a “two-wire” network the transmitter and receiver of each device are connected to a twisted pair. “Four-wire” networks have one master port with the transmitter connected to each of the “slave” receivers on one twisted pair. The “slave” transmitters are all connected to the “master”



ECM and TCM Usage for HOS Solutions

receiver on a second twisted pair. J1708 uses a “two-wire” setup to minimize the wiring complexity for the vehicle while maintaining adequate performance for message traffic.

In either configuration the microprocessors are addressable, allowing each node to be communicated to and from independently. Only a single microprocessor can drive the line at a time, so there is a delay between one node controlling the network to the next node. Two-wire 485 networks have the advantage of lower wiring costs and the ability for nodes to communicate, but is limited to half-duplex, which is slower.

This is not directly applicable to a PC which usually allows a serial (RS-232) or parallel (IEEE-128) applicable to a typical front-end HOS solution that will usually exploit the RS-232 serial standard. There are numerous commercially available adapters, a typical adapter is shown below in Figure 1 (about \$80.00) that interfaces J1708 (and usually the J1939 “high-speed” standard) to either the RS-232 serial or IEEE-1284 parallel connectors common in PC’s.



Figure 1 – Typical RS232 Serial to J1708 (RS-485) Adapter

The use of J1708 will probably not cause problems for HOS solutions as there are numerous hardware options for the various classes of solutions discussed (see Items 28-45 in the Bibliography).

2.1.2 SAE J1587 - Electronic Data Interchange Between Microcomputer Systems in Heavy-Duty Vehicle Applications

The other “low-speed” solution SAE specification is, SAE J1587, that covers the discrete messages, 13 of which this study has identified as relevant for HOS solutions. These 13 messages return both text and numeric data which are encoded using widely accepted standards. The messages themselves are uniquely identified by the Parameter Identification Number (PID).

The next three sections cover the encoding standards, MID, and lists the 13 PID to yield a list of the 13 messages and their relevance to HOS solutions.

2.1.2.1 J1587 Text Encoding uses the ASCII Extended Character Set (ISO Latin 1)

J1587 uses the American Standard Code for Information Interchange (ASCII) character set at 1 byte for each character. This was adopted internationally by the International Standards Organization (ISO) as ISO 8859-1, which is also known as the ISO Latin 1 character set.

The ASCII character set was developed at the beginning of the computer age to form a common set of characters. There are 128 standard characters, 32 of which are non-printing control characters, the rest being letters, numbers, mathematical symbols, and punctuation marks.

All 8 bits of the single byte are available to describe each character and that implies, from the computers point of view, 2^8 in base 2 or 256 in base 10, or 256 possible characters. As



ECM and TCM Usage for HOS Solutions

computers took over much of the information processing in the 1950's and forward the initial 128 characters were not enough and the so-called "extended" ASCII set was adopted to add more arcane mathematical symbols, language specific punctuation, common fractions, commonly used Greek letters, and specialized characters for putting borders around messages – all of that using up the remaining 128 ASCII codes.

Of the 256 possible ASCII characters the J1587 does not recommend displaying the ASCII control character (0 through 32) as well as the first 32 of the extended set (128-159) and is basically limited to basic mathematical and punctuation marks as well as the upper and lower case characters and the numerals 0 through 9. Table 3, shown below, depicts the characters that are encoded for text messages.

Original ASCII Character Set (0-127)										Extended ASCII Character Set (128-255)											
	0	1	2	3	4	5	6	7	8	9		0	1	2	3	4	5	6	7	8	9
30			Sp	!	"	#	\$	%	&	,	160	Nil	¡	¢	£	¤	¥	¦	§	¨	©
40	()	*	+	,	-	.	/	0	1	170	ª	«	¬	-	®	¯	°	±	²	³
50	2	3	4	5	6	7	8	9	:	;	180	´	µ	¶	·	,	¹	º	»	¼	½
60	<	=	>	?	@	A	B	C	D	E	190	¼	¿	À	Á	Â	Ã	Ä	Å	Æ	Ç
70	F	G	H	I	J	K	L	M	N	O	200	È	É	Ê	Ë	Ì	Í	Î	Ï	Ð	Ñ
80	P	Q	R	S	T	U	V	W	X	Y	210	Ò	Ó	Ô	Õ	Ö	×	Ø	Ù	Ú	Û
90	Z	[\]	^	_	,	a	b	c	220	Ü	Ý	Þ	ß	à	á	â	ã	ä	å
100	d	e	f	g	h	i	j	k	l	m	230	æ	ç	è	é	ê	ë	ì	í	î	ï
110	n	o	p	q	r	s	t	u	v	w	240	ð	ñ	ò	ó	ô	õ	ö	÷	ø	ù
120	x	y	z	{		}	~	Nil			250	ú	û	ü	ý	þ	ÿ				

Table 3 – Extended ASCII Character Set – Amended for use with J1587

Characters and their decimal (Base 10) codes can be identified by picking the 10's multiplier by row with the 1's digit by column. For example, to find the character with the ASCII code 65 go to the "60" rows then over to the column with the "5" which correctly yields an upper case "A".

Many of the messages will return numeric values, either integer or real numbers and the next two sections relate the standards used as well as the minima and maxima that can be encoded.

2.1.2.2 J1587 Integer Numeric Encoding

For integer values like time slices (number of seconds, month number, etc.) integer encodings are used. J1587 supports the three Integer format that stores values in 1, 2, or 4 bytes of a message record. These values can be either "signed" or "un-signed".

Signed values can be either positive or negative while unsigned values can be interpreted as either always positive or negative from a logical perspective, although unsigned integers are frequently interpreted as having positive values.



ECM and TCM Usage for HOS Solutions

The more bytes used for storage the greater the value that can be stored. J1587 follows the standard Integer conventions with slight differences in the names used. The 1 byte short integer, 2 byte integer, and 4 byte long integer are all used. Table 4, shown below shows the signed and unsigned short, regular, and long integers whose values can be decoded from J1587 messages.

J1587 Name	PC Name	#Bytes	Min Val	Max Val	Range
Unsigned Short Integer (Uns/SI)	Byte	1	-127	127	254
Signed Short Integer (S/SI)		1	0	255	255
Unsigned Integer (Uns/I)	Integer	2	-32767	32767	65534
Signed Integer (S/I)		2	0	65535	65535
Unsigned Long Integer (Uns/LI)	Long Integer	4	-2147483647	2147483647	4294967294
Signed Long Integer (S/LI)		4	0	4294967295	4294967295

Table 4 – J1587 Integer Encoding Nomenclature and Minima/Maxima

Message Data about dates and time which have unsigned values from 0-60 (seconds and minutes), 0-24 (hours) can use the 1 Byte encoding to save space while time measures like days (0-366) and years (0 to a practical limit much less than 65535) can use the 2 Byte encoding.

The next section covers the real numbers that are used in the messages.

2.1.2.3 J1587 Floating Point Numeric Encoding

Real or floating point numbers are also supported for values that require whole and fractional values from message data. J1587 follows the IEEE 754 standard for floating point arithmetic. The single and double precision encodings are used in J1587 which can respectively store values with either 7 or 15 place mantissa and exponents ranging from -45 to 38 and -324 to 308. This is more than enough for values measured in the various mechanical systems in HD vehicles.

As with all floating point numbers the use of either the single or double precision encoding depends primarily on the number of places of accuracy. It is unlikely that a value greater than 10^{38} or a fraction less than 10^{-45} will need to be measured and inserted into the data stream. In general good engineering practice defines units of measure with exponent shifters (milli-, micro-, nano-, etc.) to yield easy to record and communicate numbers.

A good example of this is the bit time mentioned earlier which was expressed as 104.17 msec (milliseconds) not 0.00010417 seconds. The 104.17 number is much more comprehensible if you understand what 1 millisecond represents. So for J1587 data the use of either the single or double precision encoding will depend on the accuracy required.



ECM and TCM Usage for HOS Solutions

This has to do with the mantissa, or the number of significant digits. Because an exponent is used, the range of non-zero digits is all that's needed to make the decision. Using the bit time again as an example the full number is:

0.00010417 seconds, which in scientific notation is 1.0417E-04, which has the significant digits 10417, or a mantissa of 5, is less than the single precision mantissa of 7 digits, making it acceptable for HOS data records

Table 5, shown below gives the minima and maxima for both positive and negative numbers for both the single and double precision encodings. The J1587 messages that require floating point data each specify which encoding will be used.

J1587 Name	PC Name	#Bytes	Min Val	Max Val	
Single-Precision Floating-Point	Single	4	-3.402823E38	-1.401298E-45	Neg
			1.401298E-45	3.402823E38	Pos
Double-Precision Floating-Point	Double	8	-1.79769313486231E+308	-4.94065645841247E-324	Neg
			4.94065645841247E-324	1.79769313486232E308	Pos

Table 5 – J1587 Floating Point Encoding Nomenclature and Minima/Maxima

The next section denotes the HOS-related MID from J1587.



ECM and TCM Usage for HOS Solutions

2.1.2.4 J1587 Message Identification Numbers (MID)

Table 6 below has the active MIDs for J1587 with HOS-related item in **BOLD**.

MID	Name	MID	Name	MID	Name
0 to 127	Defined by SAE J1708 (SEE Table 1)	169	Tires, Trailer #3	211	Smart Card Terminal
128	Engine #1	170	Electrical	212	Mobile Data Terminal
129	Turbocharger	171	Driver Info Center	213	VCH Touch Screen
130	Transmission	172	Off-board Diag #1	214	Silent Alarm Unit
131	Power Takeoff	173	Engine Retarder	215	Surveillance Microphone
132	Axle, Power Unit	174	Cranking/Starting System	216	Lighting Control Admin Unit
133	Axle, Trailer #1	175	Engine #2	217	T/T Bridge, Tractor Mounted
134	Axle, Trailer #2	176	Transmission, Additional	218	T/T Bridge, Trailer Mounted
135	Axle, Trailer #3	177	Particulate Trap System	219	Collision Avoidance Sys
136	Brakes, Power Unit	178	Vehicle Sensors to Data Converter	220	Tachograph
137	Brakes, Trailer #1	179	Data Logging Computer	221	Driver Information Center #2
138	Brakes, Trailer #2	180	Off-board Diags #2	222	Driveline Retarder
139	Brakes, Trailer #3	181	Comm Unit—Satellite	223	Transmission Shift Console
140	Instrument Cluster	182	Off-board Prog Station	224	Parking Heater
141	Trip Recorder	183	Engine #3	225	Weighing Sys, Axle Grp #1
142	Vehicle Mgmt System	184	Engine #4	226	Weighing Sys, Axle Grp #2
143	Fuel System	185	Engine #5	227	Weighing Sys, Axle Grp #3
144	Cruise Control	186	Engine #6	228	Weighing Sys, Axle Grp #4
145	Road Speed Indicator	187	Vehicle Mgmt System #2	229	Weighing Sys, Axle Grp #5
146	Cab Climate Control	188	Vehicle Mgmt System #3	230	Weighing Sys, Axle Grp #6
147	Cargo Refrig/Heating Trailer #1	189	Vehicle Head Signs	231	Comm Unit—Cellular
148	Cargo Refrig/Heating Trailer #2	190	Refrigerant Management Protection and Diagnostics	232	Safety Restraint System
149	Cargo Refrig/Heating Trailer #3	191	Vehicle Location Unit Differential Correction	233	Intersection Preemption Emitter
150	Suspension, Power Unit	192	Front Door Status Unit	234	Instrument Cluster #2
151	Suspension, Trailer #1	193	Middle Door Status Unit	235	Engine Oil Control System
152	Suspension, Trailer #2	194	Rear Door Status Unit	236	Entry Assist Control #1
153	Suspension, Trailer #3	195	Annunciator Unit	237	Entry Assist Control #2
154	Diag Systems, Power Unit	196	Fare Collection Unit	238	Idle Adjust System
155	Diag Systems, Trailer #1	197	Passenger Counter Unit #1	239	Passenger Counter Unit #2
156	Diag Systems, Trailer #2	198	Schedule Adherence Unit	240	Passenger Counter Unit #3
157	Diag Systems, Trailer #3	199	Route Adherence Unit	241	Fuel Tank Monitor
158	Electrical Charging System	200	Env Monitor Unit Aux Cab Climate Control	242	Axles, Trailer #4
159	Proximity Detector, Front	201	Vehicle Status Points Mon	243	Axles, Trailer #5
160	Proximity Detector, Rear	202	High Speed Comm	244	Diag Systems, Trailer #4
161	Aerodynamic Control Unit	203	Mobile Data Terminal Unit	245	Diag Systems, Trailer #5
162	Vehicle Navigation Unit	204	Vehicle Proximity, Right	246	Brakes, Trailer #4
163	Vehicle Security	205	Vehicle Proximity, Left	247	Brakes, Trailer #5
164	Multiplex	206	Base Unit (Radio Gateway)	248	Fwd Road Image Processor
165	Comm Unit—Ground	207	SAE J1708 Drivetrain Link	249	Body Controller
166	Tires, Power Unit	208	Maintenance Printer	250	Steering Column Unit
167	Tires, Trailer #1	209	Vehicle Turntable	251-	Reserved to be assigned
168	Tires, Trailer #2	210	Bus Chassis ID Unit	255	

Table 6 – J1587 MIDs – HOS-related MIDs in **BOLD**



ECM and TCM Usage for HOS Solutions

There are 24 MID's that could have direct HOS messages in the table on the previous page. They are condensed in Table 7 below with a basic indication of the probable message content for HOS. Many of the rows show a generic "Multiple Data Items" for this which indicates the generic MID and the multiple PID messages could provide some combination of date-time (when), Distance Traveled, Moving/Not Moving, and/or Location Data.

MID	Name	Relavence
128	Engine #1	Moving/Not Moving and Clock Data
130	Transmission	Moving/Not Moving
132	Axle, Power Unit	Moving/Not Moving
140	Instrument Cluster	Odometer
141	Trip Recorder	Distance Traveled
142	Vehicle Mgmt System	Multiple Data Items
145	Road Speed Indicator	Moving/Not Moving
162	Vehicle Navigation Unit	Location Data
171	Driver Info Center	Multiple Data Items
176	Transmission, Additional	Moving/Not Moving
179	Data Logging Computer	Multiple Data Items
191	Vehicle Location Unit Differential Correction	Location Data
197	Passenger Counter Unit #1	Multiple Data Items
198	Schedule Adherence Unit	Multiple Data Items
199	Route Adherence Unit	Multiple Data Items
211	Smart Card Terminal	Multiple Data Items
212	Mobile Data Terminal	Multiple Data Items
220	Tachograph	Multiple Data Items
221	Driver Information Center #2	Multiple Data Items
231	Comm Unit—Cellular	Multiple Data Items
234	Instrument Cluster #2	Odometer
239	Passenger Counter Unit #2	Multiple Data Items
240	Passenger Counter Unit #3	Multiple Data Items
248	Fwd Road Image Processor	Location Data

Table 7 – J1587 HOS-related MIDs

The MID is a required part of any J1587 message field but is not strictly linked to the PID. MID's are meant to provide a set of HD vehicle subsystems that can have dedicated network nodes whose message(s) would show that MID. The messages in Appendix A of J1587 do not list the referencing MID but are tied strictly to their Parameter Identification Number.

The next section depicts a list of the thirteen J1587 messages with their associated PID's. The details for the message can be found in Section 3 of this document which lists the required HOS data with the content and details from both the "low-speed" and "high-speed" in single locations for easy comparison.



ECM and TCM Usage for HOS Solutions

2.1.2.5 J1587 Messages for HOS Solutions

J1587 uses a single character for the PID which, like the MID in J1708, allows up to 256 unique PIDs. The list has been extended to encompass another 256 PID's for a current total of 512 active messages. Each PID uniquely identifies a message and Appendix A of the J1587 document has the details for each message, what is measured, the accuracy, message priority and other items. This section of the document lists the specific messages from the "low-speed" specification but does not provide the details – those can be found in Section 3 of this document along with the "high-speed" message counterparts.

The HOS data record posed in Section 3.3.3 of the Research and Analysis on Hours of Service (HOS) Data Record Structure and Data Security Document (previously delivered to FMCSA) requires that 15 (Part 395) items have data gathered to fill the notional 24-bytes HOS data record as well as 3 additional items. The Part 395 table is re-printed below as Table 8 to form the basis of the subjects that the J1587 messages need to address. As before the data recovery method definitions in the Type Column are:

- P – Preloaded data that is stored once before the trip starts
- I – Input by the driver as Duty Status Changes or a State Border is crossed
- D – Demanded from internal sources, the date-time or location
- C – Always computed as the Miles Driven and Total Hours are time depended

#	Ref	Type	Description	J1587 PID
1	§395.15(c)(1)	I	Status Change - Driver is Off Duty	None
2	§395.15(c)(2)	I	Status Change - Driver is in Sleeper Berth	None
3	§395.15(c)(3)	I	Status Change - Driver is On Duty - Not Driving	None
4	§395.15(c)(4)	I	Status Change - Driver is On Duty - Driving	None
5	§395.15(c)(5)	D	Date-Time Group	251,252,253
6	§395.15(c)(6)	C	Total Miles Driving Today	245,509
7	§395.15(c)(7)	P	Truck/Tractor & Trailer Number	237
8	§395.15(c)(8)	P	Name of Carrier	None
9	§395.15(c)(9)	P	Main Office Address	None
10	§395.15(c)(10)	P	24-hour period starting time	None
11	§395.15(c)(11)	P	Name of Co-Driver	447,507
12	§395.15(c)(12)	C	Total Hours	245,251 252,509
13	§395.15(c)(13)	P	Shipping Doc Numbers, etc.	None
14 15	§395.15(d)(1,2)	D,I	Location – Stored as numeric codes (only requires numeric keypad for data entry versus a keyboard)	218,219,239
16	Data Security	P	Driver Identification	447,507
17	Safety Issue	C	Truck is <u>M</u> oving or <u>N</u> ot <u>M</u> oving (M/NM)	84,160
18	Tampering	C	Date-Time Group was Adjusted	None

Table 8 – Required HOS Data With Associated J1587 Messages



ECM and TCM Usage for HOS Solutions

The data stored will be secure which requires the driver be identified for authentication purposes and this has been added as a 16th item. Safety considerations also require that the truck not be moving when HOS events are initiated so a Boolean indicator about the truck moving or not moving can also be available; this has been added to the table as a 17th item. J1587 can also provide date-time adjustment events and that has been added as an 18th item. A column has been added at the right to indicate which items are available from J1587 messages and if so identifying the specific PID(s).

The numbers in the column at the right of Table eight indicate the 13 unique J1587 messages of interest. Table 9, shown below lists them sorted by the PID with the location in Appendix A of J1587 indicated at the right of the table.

#	PID	Message Name	HOS Relevance	SAE J1587 Ref Location
1	84	Road Speed	Primary datum for M/NM	A.84 - Page 71
2	160	Main Shaft Speed	Lexical AND check or backup for M/NM	A.160 Page 99
3	218	State Line Crossing	Would further automate the HOS solution in the relatively few trucks with the hardware and software to continuously compute this	A.218 Page 125
4	219	Current State and Country		A.219 Page 126
5	237	Vehicle ID Number	Could be used to verify pre-loaded data and check for a replacement tractor during the trip	A.237 Page 134
6	239	Vehicle Position	Used to directly get the Latitude and Longitude data in vehicles with an integrated GPS system	A.239 Page 135
7	245	Total Vehicle Distance	The Odometer Reading for Distance Traveled Computations to get the HOS Compliance	A.245 Page 138
8	251	Clock	The time of day for the date-time group	A.251 Page 140
9	252	Date	The day, month, and year for the date-time group	A.252 Page 141
10	253	Elapsed Time	Could be used as a backup for clock data, limited to relative measures	A.253 Page 141
11	447	Passenger Counter	Could augment and/or check pre-loaded data	A.447 Page 172
12	507	Driver Identification		A.507 Page 185
13	509	Mile Post Identification	Could augment location data but very unlikely given the number of trucks (and road infrastructure) that supports this	A.509 Page 186

Table 9 – HOS Related J1587 Messages



ECM and TCM Usage for HOS Solutions

The message formats are recommended by SAE, but may or may not have been implemented within the trucking industry. They are in the Specification and as such need to be denoted as applicable to HOS solution and be included in any future design specification. The HOS solution software would need to check the trucks “low-speed” network and exploit these messages if available thereby resulting in the most automated and tamper-proof solution.

The next section covers the “high-speed” HD vehicle network specified in SAE J1939. This network is about 30 times faster, contains 2255 messages, and offers direct analogs for most J1708 message in Table 9 as well as additional messages that could be used to further enhance HOS solutions.

2.2 “High-Speed” SAE J1939 – Gaining Ground in HD Vehicles

The J1939 “high-speed” standards were issued by SAE in April 2000, about 14 years after the J1708/J1587 “low-speed” standard. At that point in time the notion of Local Area Networks (LANs) had been well established with numerous topologies developed and in place. Bosch in Europe had been successfully using its Controlled Area Network (CAN) system (detailed in ISO 11898) in both automobiles and trucks since the early 1990’s.

J1939 uses Version 2.0B of CAN as its basis for the “high-speed” HD vehicle networks. The network topology uses the peer-to-peer notion that allows numerous controllers to be present as “nodes” on the network – much the same as in PC networks where PC’s are linked. In this case there is no data server and the controllers at the nodes each take care of their associated function, stored data, etc.

J1939 first assigned an Industry Group Code to begin the taxonomy of the messaging detailed in J1939-71. There are 5 active groups of which the first, On-Highway Equipment, encompasses the HOS solutions. The other four include Agricultural and Forestry Equipment, Construction Equipment, Marine, and Industrial and Process Control Equipment.

J1939-11 defines the protocol (based on the ISO 11898) without the message infrastructure, and is analogous to the “low-speed” J1708 specification. J1939-21 defines the message structure and is analogous to basic MIDs as defined in J1708. Other J1939 sections cover the physical architecture and network performance that have analogs in J1708.

The message structure in the J1939-71 portion is much more complex than J1587 with specific formats at the bit (versus byte for the J1708) level except for the data contents which are still defined in bytes. The data portions of the messages all adhere to the same character (ASCII ISO Latin 1) and Integer and Floating Point (IEEE 754-1985) encodings as in the “low-speed” specification. As a direct comparison there are 2255 active messages in J1939-71 versus 512 in J1587.



ECM and TCM Usage for HOS Solutions

J1939-71 messages are identified by a unique numerical value that is used for Fault Checks, called the Sspect Parameter Number (SPN). Many of these SPN's have the same value as the PID's from J1587 indicating the lower numbered messages were re-used for compatibility. In addition there is the Parameter Group Name (PGN) which, in most cases, also uniquely identifies the message; these are found in Section 5.3 of J1939-71. The PGN can, and often is, divided into individual Parameter Definitions (PDs) which hold the detailed information about the message data content and are found in Section 5.2 of J1939-71.

In all the subsequent tables, messages that point to HOS data the SPN, PGN, and PD will all be listed with a complete reference of where the message is found in J1939. This study's research indicates that J1939-71 messages are available to provide the required date-time, elapse distance, and moving-not moving parameters as well other HOS-related data not available via J1587. J1939 currently uses five message types during normal operations which are Commands, Requests, Broadcasts/Responses, Acknowledgments, and Group Functions.

HOS solutions will demand a specific datum from the vehicle's ECM (odometer reading, date/time, etc.) for which a specific value will be returned. Commands and Requests perform this function in J1939 networks and are adequate to recover the required HOS information.

Commands are destination specific and are used to cause some specific action to happen at the destination. In general this would not be used with HOS solutions where the goal is to discretely demand information from the vehicles network.

Requests are used to gather information which can be global or destination-specific, depending on the data being requested. The HOS solutions could use either as required. Central to any HOS solution's software is to be able to poll the particular vehicle and determine what data (via the messages) is available. This will vary by vehicle. Any HOS design specification should be posed so as to force the software to poll the vehicle for the available messages to automate the process as much as possible. This will also reduce the ability for others to tamper with the secured information to the maximum extent.

The last three types could be used but are not required for demanding HOS data. They are:

Broadcast/Responses can either be an unsolicited broadcast of information or a response to a Command or Request.

Acknowledgments are responses to specific commands; they may be either positive or negative

Group Functions are used for special groups of functions, such as network functions, proprietary messages, and multi-packet transport functions.



ECM and TCM Usage for HOS Solutions

The actual data content that the HOS solution demands would be extracted from the J1939-71 message and then stored in the notional HOS data record described in the Research and Analysis on Hours of Service (HOS) Data Record Structure and Data Security Document. Some J1939 messages can contain more than 8 bytes of information, a few of which may be of interest for HOS solutions. In this case the data is split into multiple data records.

The next section describes the specifics of the overall data structure and the timing limitations for HOS solutions interfacing with the “high-speed” J1939 vehicle data networks.

2.2.1 J1939-11, J1939-21, and J1939-31 Physical Network Description

The J1939-11, J1939-21, and J1939-31 portions of the overall specification describe, among other things, the physical network and are analogous to the J1708 “low-speed” standard. They describe the physical network components and software protocols used to move the message data among the nodes.

The network uses a shielded twisted pair wire that is terminated at 120 ohms. All the devices, on the network tap in to the wire with simple connectors, forming the nodes for the network. This is similar to LAN’s with PC’s but in this case there is no server to control data flow traffic. The individual controllers contain firmware that controls the peer-to-peer connections and allow the network to function.

The J1939-11 and J1939-31 portions of the specification detail have specific connector and wiring techniques for the HD vehicle implementations. There is no direct PC connection but as in the “low-speed” situation there are numerous hardware and software options. Figure 2 below depicts a PDA solution on the left and a PC software solution (Hercules from the Dearborn Group) on the right that illustrates the ease of recovering messages.

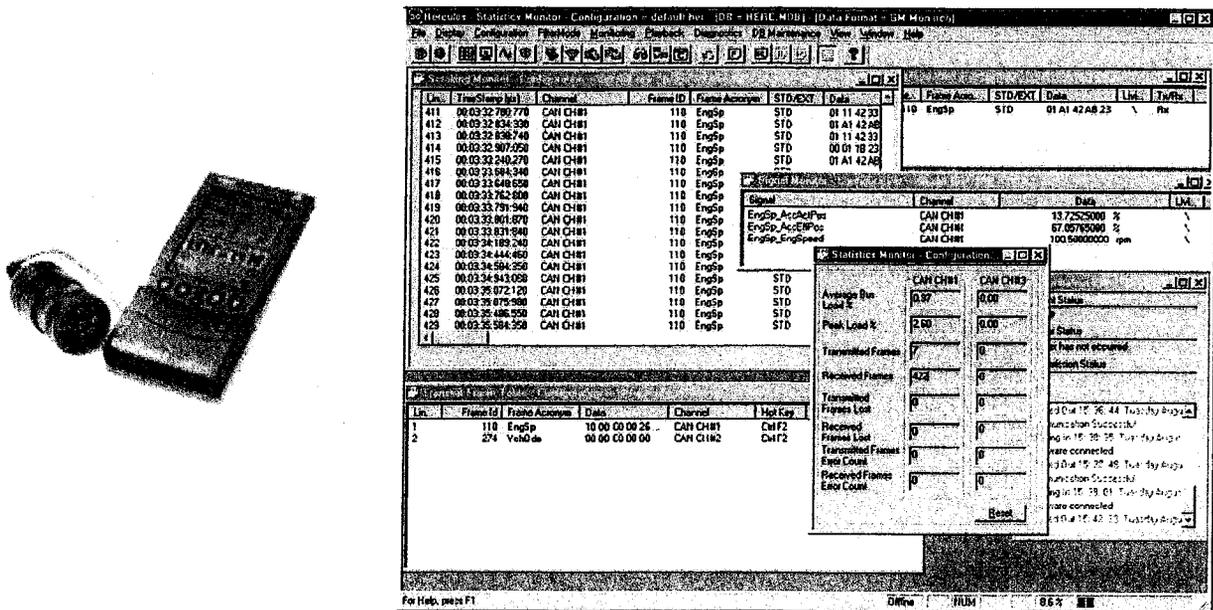


Figure 2 – Typical J1939 Hardware and Software



ECM and TCM Usage for HOS Solutions

In general the use of J1939 allow more HOS solution automation than their “low-speed” counterparts. There are already numerous hardware and software products that are J1939 compliant; see Items 28-45 in the Bibliography for some examples.

2.2.1.1 Overall Data Structure and Timing Limitations

J1939 is at least 30 times faster than the J1708/J1587 “low-speed” network and as such does not employ a standard bit time as in J1708 because the clock-speed of the individual network device can vary. These devices usually employ at least a 16 MHz clock speed in the nodes which yields about 250 nsec as opposed to the 104 msec in J1708 (about 240,000 times faster as the worst case).

Furthermore the J1939 does not employ the UART notion of adding 2 bits to each character so there is 1 byte per character as in almost all the rest of the computing world. Factoring in all the handshake protocols and other housekeeping tasks that peer-to-peer networks employ, the data throughput yields a minimum of 250,000 bits per second, which in turn implies 31,250 characters per second or about 1,666 messages per second using the J1939 record.

This is about $31.250/45$ or about 700 times faster than the low-speed specification, and is perfectly adequate for HOS solutions.

2.2.2 SAE J1939-71 – Vehicle Application Layer for Messages

The J1939-71 portion of the “high-speed” solution covers the discrete messages, 26 of which this study has identified as relevant for HOS solutions. These 26 messages return both text and numeric data which are encoded using widely accepted standards, in fact the same ones as are used in the older “low-speed” J1587 specification.

The messages are uniquely identified and cross-referenced by the three pieces of information (the SPN, PGN, and PD numbers mentioned earlier) versus one in J1587. The next three sections cover the encoding standards, which are the same as in J1587.

2.2.2.1 J1939 Text Encoding uses the ASCII Extended Character Set (ISO Latin 1)

J1939-71 messages with character content use the same ASCII extended character set with the excluded control characters as in J1587. Refer to Section 2.1.2.1 of this document for the details.

2.2.2.2 J1939 Integer Numeric Encoding – Same as J1587

J1939-71 messages with Integer content use the same 1, 2, and 4 byte encodings as in J1587. Refer to Section 2.1.2.2 of this document for the details.

2.2.2.3 J1939 Floating Point Numeric Encoding – Same as J1587

J1939-71 messages with Floating Point content use the same single and double precision encodings as in J1587. Refer to Section 2.1.2.3 of this document for the details.

The next section relates the location in the J1939 document for the SPN, PGN, and PD message descriptors.



ECM and TCM Usage for HOS Solutions

2.2.2.4 J1939 Specific Message Identification Parameters

There are three data that specify a message and are reflected in Table 11 that specifies the J1939 messages of interest for HOS solutions. The three datum's are:

Suspect Parameter Number (SPN) – Found in Table C-1 of the J1939 document from Page 53 to 117 and range in value from 1 to 2255. There is a unique number for each message with a cross-reference to the PGN that in-turn specifies the specific contents of the messages.

Parameter Group Name Number (PGN) – These are 5 digit integers that identify the group of PD's that comprise a message. Section 5.3 of J1939-71 from page 369 to 429 of the J1939 document contains the PGN's.

Parameter Description(s) (PDs) in paragraph in Section 5.2 of J1939-71 describe each PGN data item and has the details for the message contents. The Section 5.2 of J1939-71 PGN description is found at page 233 to 368.

There is no analogy to the MID's in both J1708 and J1587 from the "low-speed" in J1939. The next section depicts a list of the twenty-six J1939-71 messages with their associated SPNs, PGNs, and PDs. The details for the message can be found in Section 3 of this document which lists the required HOS data with the content and details from both the "low-speed" and "high-speed" in single locations for easy comparison.

2.2.2.5 J1939 Messages for HOS Solutions

This section of the document lists the specific messages from the "high-speed" specification but does not provide the details – those can be found in Section 3 of this document along with the "low-speed" message counterparts. The HOS data record posed in Section 3.3.3 of the Research and Analysis on Hours of Service (HOS) Data Record Structure and Data Security Document requires that the fifteen items under Section 395.15 of the FMCSRs and 2 related items have data gathered to fill the notional 24-bytes HOS data record.

The driver identification should be stored as secure data. That data is to be provided for driver authentication and has been added as a 16th data item in Table 10 on the next page. Safety considerations also require that the truck not be moving when HOS entries are made so a Boolean indicator about the truck moving or not moving also needs to be available; this has been added to the same table as a 17th item. J1939 can also provide date-time adjustment events and that has been added as an 18th item. A column has been added at the right to indicate which items are available from J1587 messages, and if so, identifying the specific PID(s).

The Part 395 table is re-printed on the next page as Table 10 to form the basis of the subjects that the J1939-71 messages need to address. The data recovery methods in the Type Column are:

- P – Preloaded data that is stored once before the trip starts
- I – Input by the driver as Duty Status Changes or a State Border is crossed
- D – Demanded from internal sources, the date-time or location
- C – Always computed as the Miles Driven and Total Hours are time depended



ECM and TCM Usage for HOS Solutions

#	Ref	Type	Description	SPN	PGN
1	§395.15(c)(1)	I	Status Change - Off Duty	1612	65132
2	§395.15(c)(2)	I	Status Change - Sleeper Berth	1613	
3	§395.15(c)(3)	I	Status Change - On Duty - Not Driving	1615	
4	§395.15(c)(4)	I	Status Change - On Duty - Driving	1616	
5	§395.15(c)(5)	D	Date-Time Group	959,960 961,962 963,964	65254
6	§395.15(c)(6)	C	Total Miles Driving Today	245	65248
7	§395.15(c)(7)	P	Truck/Tractor & Trailer Number	237	65260
8	§395.15(c)(8)	P	Name of Carrier	None	None
9	§395.15(c)(9)	P	Main Office Address	None	None
10	§395.15(c)(10)	P	24-hour period starting time	None	None
11	§395.15(c)(11)	P	Name of Co-Driver	1626	65131
12	§395.15(c)(12)	C	Total Hours	245 959,960 961,962 963,964	65248 65254
13	§395.15(c)(13)	P	Shipping Doc Numbers, etc.	None	None
14 15	§395.15(d)(1,2)	D,I	Location – Stored as numeric codes (only required numeric keypad for data entry versus keyboard)	584 585	65267
16	Data Security	P	Driver Identification	1625	65131
17	Safety Issue	C	Truck is <u>M</u> oving or <u>N</u> ot <u>M</u> oving (M/NM)	84 160 516 1611	65265 None None 65132
18	Possible Tampering	C	Date-Time Group was Adjusted	1603,1604 1605,1606 1607,1608	54528

Table 10 – Required HOS Data With Associated J1587 Messages

The numbers in the 2 right-most columns of Table 10 indicate the SPN and PGN for the 26 unique J1939 messages of interest. Table 11, shown on the next page lists them by SPN with the locations in Specification Appendix C (SPN), Sections 5.3 (PGN), and 5.2 (PD) indicated.



ECM and TCM Usage for HOS Solutions

#	SPN	PGN	Message Name	HOS Relevance	PGN Para/Pg	PD Para/Pg
1	84	65265	Wheel-Based Road Speed	Backup datum for M/NM determination	5.3.031/382	5.2.5.012/237
2	160	None	Main Shaft Speed	Lexical AND check or backup for M/NM	None	5.2.5.054/284
3	237	65260	Vehicle ID Number	Used to verify pre-loaded data and check for a new tractor during the trip	5.3.026/380	5.2.5.087/291
4	245	65248	Total Vehicle Distance	The Odometer Reading for Distance Traveled Computations to get the HOS Compliance	5.3.014/374	5.2.5.051/283
5	959	65254	Clock Seconds	Used for Date-Time Recovery	5.3.020/378	5.2.5.093/292
6	960		Clock Minutes			5.2.5.094/292
7	961		Clock Hours			5.2.5.110/297
8	962		Clock Day			5.2.5.111/297
9	963		Clock Month			5.2.5.112/297
10	964		Clock Year			5.2.5.113/298
11	516	None	Ground-based Road Speed	Radar Speedometer, backup for M/NM if Equipped	None	5.2.1.011//237
12	584	65267	Latitude	Use for location data is GPS integrated into the network	5.3.033/383	5.2.5.086/290
13	585		Longitude			5.2.5.087/290
14	1603	52548	Adjust Clock Seconds	Used for Date-Time Tampering Detection	5.3.144/429	5.2.5.288/338
15	1604		Adjust Clock Minutes			5.2.5.289/338
16	1605		Adjust Clock Hours			5.2.5.290/338
17	1606		Adjust Clock Day			5.2.5.291/338
18	1607		Adjust Clock Month			5.2.5.292/339
19	1608		Adjust Clock Year			5.2.5.293/339
20	1611	65132	Drive Recognize	Direct Readout of M/NM, use as Primary	5.3.143/428	5.2.6.078/361
21	1612		Driver 1 Work State	These messages contain analogs to HOS duty status change codes. Could be used to eliminate installed hardware in the truck		5.2.1.012/237
22	1613		Driver 2 Work State			
23	1615		Driver Card 1	Could augment and/or check pre-loaded data and Duty Status Change Events		5.3.145/429
24	1616	Driver Card 2				
25	1625	65131	Driver ID 1	5.3.145/429	5.2.5.287/338	
26	1626		Driver ID 2			

Table 11 – HOS Related J1939 Messages



ECM and TCM Usage for HOS Solutions

The message formats are specified by SAE but may or may not have been implemented within the trucking industry. They are in the Specification and as such need to be denoted as applicable to HOS solution and be included in any future design specification. The HOS solution software would need to check the trucks “low-speed” network and exploit these messages if available thereby resulting in the most automated and tamper-proof solution.

The next section of the document covers the specific data required for HOS solutions and what is available from the “low-speed” and “high-speed” solutions based on Tables 8, 9, 10, and 11.



ECM and TCM Usage for HOS Solutions

SECTION 3 –ECM MESSAGE DETAILS FOR HOS SOLUTIONS

The last section introduced the notion of 18 datums that are needed for effective HOS solutions. Section 2.1 of this document addressed them for the J1708/J1587 “low-speed” vehicle network and Section 2.2 for J1939 “high-speed” vehicle networks. The Part 395 table is re-printed again below as Table 12 indicate which areas are addressed by recoverable message data for either of the network types. As before the data recovery method definitions in the Type Column are:

- P – Preloaded data that is stored once before the trip starts
- I – Input by the driver as Duty Status Changes or a State Border is crossed
- D – Demanded from internal sources, the date-time or location
- C – Always computed as the Miles Driven and Total Hours are time depended

#	Ref	Type	Description	Low Spd	High Spd
1	§395.15(c)(1)	I	Status Change - Driver is Off Duty		X
2	§395.15(c)(2)	I	Status Change - Driver is in Sleeper Berth		X
3	§395.15(c)(3)	I	Status Change - Driver is On Duty - Not Driving		X
4	§395.15(c)(4)	I	Status Change - Driver is On Duty - Driving		X
5	§395.15(c)(5)	D	Date-Time Group	X	X
6	§395.15(c)(6)	C	Total Miles Driving Today	X	X
7	§395.15(c)(7)	P	Truck/Tractor & Trailer Number	X	X
8	§395.15(c)(8)	P	Name of Carrier		
9	§395.15(c)(9)	P	Main Office Address		
10	§395.15(c)(10)	P	24-hour period starting time		
11	§395.15(c)(11)	P	Name of Co-Driver	X	X
12	§395.15(c)(12)	C	Total Hours	X	X
13	§395.15(c)(13)	P	Shipping Doc Numbers, etc.		
14 15	§395.15(d)(1,2)	D,I	Location – Stored as numeric codes (only requires numeric keypad for data entry versus a keyboard)	X	X
16	Data Security	P	Driver Identification	X	X
17	Safety Issue	C	Truck is <u>M</u> oving or <u>N</u> ot <u>M</u> oving (M/NM)	X	X
18	Tampering	C	Date-Time Group was Adjusted		X

Table 12 – Low and High Speed Messages for HOS Data Items

Note that the newer J1939 specification can provide more information to augment an HOS solution. Of the 18 items there are 4 (8, 9, 10, and 13) that are not provided by either network type which is acceptable as these items are pre-loaded before the trip begins. There are also data items that the “high-speed” network can provide but the “low-speed” network can not. These are items 1,2,3,4, and 18 which address Duty Status Changes and clock tampering.



ECM and TCM Usage for HOS Solutions

If these messages are supported by a particular J1939 compliant vehicle they should be exploited to automate the HOS solution to the maximum extent possible. This will make the HOS process more transparent to the driver(s) while minimizing the susceptibility for tampering.

HOS solutions could use 7 types of data, all discretely demanded ECM or TCM. They are:

1. Demanding the Date-Time for HOS record timestamps and time-related computations
2. Demanding datum's to determine whether the truck is moving or not moving
3. Demanding the Odometer reading for distance calculations
4. Demanding location data for required position computations
5. Demanding data to check or augment pre-loaded information as the trip progresses
6. Demanding Clock adjustments to minimize tampering (J1939 Only)
7. Demanding Driver Status Information to automate the Status Change Events (J1939 only)

The next 7 sections go though each of the above with the appropriate details from the “low-speed” and/or “high-speed” messages as available.

3.1 Demanding a Date-Time Group – Obtainable From Either Specification but J1939 More Tamper-resistant

Central to the HOS data record is the ability to discretely demand the date and time. The time recovered is used to timestamp the record and to provide the information to compute the hours driven for HOS compliance. Both the “low-speed” and “high-speed” vehicle networks have directly accessible messages to accomplish this.

The J1587 has two messages, one for the date, the other for the time while the J1939-71 separates the date-time group into six parts; hours, minutes, and seconds for the time and day, month, and year for the Date. The next two sections show the details.

3.1.1 J1587 or J1939-71 Date Messages

The J1587 message provides 3 unsigned Short Integers (1 Byte each) that define the date. The three Short Integers represent the day, month, and year respectively. The same resolution was applied in both network types to yield a ¼ day resolution with direct use for years and months. Years are inherently greater than the maximum 255 value of an Unsigned Short Integer and this measurement uses an offset from 1985. So the value recovered for the year has 1985 added to it to yield the correct year.

J1939-71 splits the Short Integers into three 1 Byte messages with the same nomenclature and year offset of 1985. Table 13 below summarizes the results.

Measure	Range	Resolution	Encoding	J1587 Ref	J1939-71 Ref
Year	1985 - 2235	1	US Short Int	A.252 Page 141	5.2.5.113 – Pg 298
Month	1 -12	1	US Short Int		5.2.5.112 – Pg 297
Day	0.25- 31.75	.25	US Short Int		5.2.5.111 – Pg 297

Table 13 – Date Measurement Message Details



3.1.2 J1587 or J1939-71 Time Messages

The J1587 message provides 3 unsigned Short Integers (1 Byte each) that define the time. The three Short Integers represent the seconds, minutes, and hours respectively. Short Integers can yield values from 0 to 255 so the second's range needs to be at least 60. This allows a ¼ second resolution ($255 * .25 = 63.75$ seconds which is greater than 60). Since there are 60 minutes in an hour and 24 hours in a day, the Short Integers for these fields can be used directly.

J1939-71 splits the Short Integers into three 1 Byte messages but retains the same resolution of ¼ of a second. The result is that the time can be measured by either network type to a ¼ second accuracy which is acceptable for HOS solutions. Table 14 below summarizes the results.

Measure	Range	Resolution	Encoding	J1587 Ref	J1939-71 Ref
Hour	0 - 23	1	US Short Int	A.251 Page 140	5.2.5.110 – Pg 297
Minute	0 -59	1	US Short Int		5.2.5.094 – Pg 292
Second	0- 59.75	.25	US Short Int		5.2.5.093 – Pg 292

Table 14 – Time Measurement Message Details

3.1.3 J1587 Backup Date-Time Group via Elapsed Time Message – No backup in J1939-71

The J1587 “low-speed” network can yield an elapsed time which could be demanded to indirectly check clock resets. The elapsed time message in J1587 in A.253 usually provides 4 Unsigned Short Integers that provide the elapsed days, hours, minutes, and seconds since the last reset. The reset event is not demandable but getting both the elapsed time and clock messages during HOS record formations could allow a discontinuity between them be to logged as suspicious. It would not directly indicate tampering but would flag potential problems.

The use of the Unsigned Short Integer and the ¼ second resolution is the same as described above. Table 15 below summarizes the results.

Measure	Range	Resolution	Encoding	J1587 Ref
Day	0 – 255	1	US Short Int	A.251 Page 140
Hour	0 - 23	1	US Short Int	
Minute	0 -59	1	US Short Int	
Second	0- 59.75	.25	US Short Int	

Table 15 – Elapsed Time Measurement Message Details

3.2 Moving/Not-Moving Related Messages – Numerous Alternatives

The Research and Analysis on Hours of Service (HOS) Data Record Structure and Data Security Document Deliverable discussed requiring drivers to be stopped when changing Driver Status, but allow State Border Crossing Status Changes while moving in vehicles equipped with an integrated GPS system. These “rules” require that the HOS solution be able to demand whether the vehicle is Moving or Not Moving (M/NM).



ECM and TCM Usage for HOS Solutions

The “Drive Recognize” message can be utilized if available in J1939 networked vehicles for a direct answer for M/NM. If the direct reading is not available or the truck uses a “low-speed” network, the M/NM datum can be recovered indirectly with the Speedometer (No speed indicates No Motion) reading. As a check and/or backup the Transmission Main Shaft Rotational Speed (0 RPM’s indicates No Motion) can be used. The next three sections cover these messages.

3.2.1 J1939-71 Drive Recognize – Direct Measure on “High-Speed” Networks

The J1939 has a PGN for Tachographs that returns an 8 byte message with numerous datums. The 7th and 8th bit of the first byte of this message indicates whether the vehicle is moving or not. The two possible responses are shown in Table 16 below.

PGN	Byte	Bit 7	Bit 8	Indicates	J1939-71 Ref
TCO1	1	0	0	Not Moving	5.2.1.012 – Pg 237
TCO1	1	0	1	Moving	5.3.143 – Pg 428

Table 16 – Direct M/NM Measurement Message Details

3.2.2 J1587 or J1939-71 Wheel-Based Road Speed – Primary M/NM Source

The best way to determine whether the vehicle is moving or not in “low-speed” networks is to recover the Speedometer value, a non-zero value indicating motion. Almost all vehicles will have this feature on their internal networks, making it an excellent way to set the M/NM portion of the HOS record. Since we are only interested in a zero or non-zero response the range of 0-127.5 mph in J1587 networks is fully acceptable.

The J1939 “high-speed” networks use a 2 byte unsigned integer, allowing values up to 65535 to be returned with a correspondingly higher resolution (about 1/412 mph/bit or about 200 times higher than the “low-speed” equivalent). The maximum speed that can be measured is somewhat higher but much more accurate, although many commercially available sensors will resolve 1/412 of a mph based on measuring the rotational speed of a shaft or wheel. The only interest is in zero or non-zero messages so this output is acceptable. Table 17 shows the results for both network types.

Measure	Range	Resolution	Encoding	J1587 Ref
Speed (mph)	0 – 127.5	.5	US Short Int	A.84 Page 71
Measure	Range	Resolution	Encoding	J1939-71 Ref
Speed (mph)	0 -155.87	1/412.238 Mph/bit gain	US Integer	5.2.5.012 – Pg 237 5.3.031 – Pg 382

Table 17 – Road Speed Measurement Message Details



3.2.3 J1587 or J1939-71 Main Shaft Speed - Backup M/NM Source

Both networks need a backup method of determining M/NM and the rotational speed for the main shaft in the transmission can be used directly. Like the speedometer a zero rotational speed indicates no motion. This message uses an unsigned integer and a resolution of ¼ of an RPM in “low-speed” networks and 1/8 of an RPM in “high-speed” networks, allowing rotational speeds of over 8,000 RPM. Since we are only interested in zero or non-zero this message’s output is acceptable. Table 18 shows the results.

Measure	Range	Resolution	Encoding	J1587 Ref
Rotational Speed (RPM)	0 to 8031.875	.125	US Integer	J1939/5.2.5.054 Page 284
Rotational Speed (RPM)	0 to 16,383.75	.25	US Integer	J1587/A.160 Page 99

Table 18 – Main Shaft Rotational Speed Measurement Message Details

3.3 Demanding the Odometer Reading

To correctly compute HOS compliance periodic readings of the distance traveled are required. Calculating the difference, combined with date-time and Part 395 rules, yields the result. Both the “low-speed” and “high-speed” network types can return the total distance traveled by the vehicle.

3.3.1 J1587 or J1939-71 for Total Vehicle Distance

Both network types use unsigned Long Integers for this with the “low-speed” resolution at 1/10th of a mile yielding a range out to over 429 million miles. The “high-level” network uses a .125 km resolution which translates to 0.201 miles which translates to a range to over 327 million miles.

The interest is in the resolution than the maximum value that can be handled by the message. For HOS compliance the difference between odometer readings will need to be calculated to determine the accuracy driving the overall tolerance on the primary time and distance ingredients. The resolutions of 0.10 and 0.201 miles for the network types are much less than the threshold maximum driving distances mandated in Part 395 and should be acceptable. Table 19 shows the results for both network types.

Measure	Range	Resolution	Encoding	References
Total Dist (Mi)	0 - 429,496,729.5	0.10	US Long Int	J1587/A.84 Page 71
Total Dist (Mi)	0 - 327,080,569.4	0.201	US Long Int	J1939-71/5.2.5.012 – Pg 237 J1939-71/5.3.031 – Pg 382

Table 19 – Road Speed Measurement Message Details



3.4 Location-Related Messages for HOS Solutions on Vehicles with Integrated GPS Systems

The two network types offer a number of location-dependent messages. They are only available if the vehicle has the GPS or other externally networked system integrated into the vehicle's "low-speed" or "high-speed" network. The basic message that could be demanded in either network type provides the latitude and longitude of the location when demanded. This is analogous to making a separate cabled connection from the HOS solution's hardware direct to the GPS receiver.

GPS receivers broadcast date-time, latitude, longitude, and altitude; which could be used for HOS location data. Using the ECM as a pass-through device will yield the location data with the data already transformed to angle measures for latitude and longitude.

There are 3 additional messages, all defined in the J1587 "low-speed" network, that could also be used to augment HOS data directly. The A.218 message provides the date-time and State (2-character Postal Code) when this occurs. The A.219 message does the same thing but can discretely provide the State code (no date-time group). These can be used to provide some of the data inputted when driver status changes.

These messages will not provide the nearest Named Place Code or State Border Crossing Location Code as described in the Research and Analysis on Hours of Service (HOS) Data Record Structure and Data Security Document but could provide some of the input data. It is doubtful that most vehicles will contain the on-board computing and database resource to take a GPS input and compute the State Codes when these messages are requested.

The Module 3 Research and Analysis on Using Geo-Referenced Place Names in Hours of Service Solutions and Module 4 Research and Analysis on Using State Border Crossing Data in HOS Solutions indicate that this automation could be easily incorporated, making the use of the A.218 and A.219 messages less important. It is probably more efficient to demand the latitude and longitude from the ECM as the primary source or a cabled connection to a GPS receiver as a backup and let the HOS solution compute the entire suite of data needed for the HOS data record.

An additional record for milepost sensors could also be used to provide additional data about the vehicles location but this is questionable given the real-world infrastructure that exists. The next section shows the basic latitude and longitude messages with the three sections following the specialized "low-speed" messages.

3.4.1 J1587 and J1939-71 for Direct Location Data

Both network types can directly provide the latitude and longitude and use long integers. These measures are really floating point numbers and very small resolutions are used to yield decimal degrees for the numbers after decoding.



ECM and TCM Usage for HOS Solutions

The “low-speed” message provides a 10 byte output of which the first and second 4 byte parts are signed long integers with the latitude and longitude respectively. They both use a 1/1,000,000 degree/bit resolution which allows the sign of the number to indicate north or south latitude and east or west longitude. This yields +/- 2147 degrees for either latitude or longitude which is sufficient for a HOS Solution.

The “high-speed” standard uses unsigned long integers with a resolution of 1/10,000,000 degree/bit and a -120 degree offset for more precision. This yields +/- 211 degrees for either latitude or longitude which again, is sufficient for a HOS Solution.

Because of the long integers 10 place mantissa the precision of the measured number after conversion to decimal degrees is significantly greater than the accuracy the GPS satellite method of measurement can provide, making these encoding acceptable for HOS solutions. Table 20 below shows the results for both network types

Measure	Byte Pos	Range	Resolution	Encoding	J1587 Ref
Latitude (DD)	1 to 4	-2147.483648 to 2147.483647	1.0E ⁻⁶	S Long Int	A.239 Page 135
Longitude (DD)	5 to 8				
Measure	#Bytes	Range	Resolution	Encoding	J1939-71 Ref
Latitude (DD)	4	-210.000000 to 211.108121	1.0E ⁻⁷	US Long Int	5.2.5.085 – Pg 290
Longitude (DD)	4				5.2.5.086 – Pg 290

Table 20 – Road Speed Measurement Message Details

3.4.2 J1587 for State Border Crossings – Only on “Low-Speed” Networks with Sophisticated GPS and On-Board Databases or External Communications

This specialized message could be available in some vehicles and would provide the “From” and “To” state as well as a date-time group accurate to +/- 1 minute. This does not represent all the required data but could save some processing. Table 21 below has the results.

Measure	Byte Pos	Range/Ref	Resolution	Encoding	J1587 Ref
Day	1	.25 to 31.75	.25	US Short Int	A.218 Page 125
Month	2	1 to 12	1		
Year	3	1985 to 2235	1		
Minute	4	0 to 59	1		
Hour	5	0 to 23	1		
“From” State	6-8	Postal Code 65		3 Char Max for each	
“From” Country	9-11	ISO 3166			
“To” State	12-14	Postal Code 65			
“To” Country	15-17	ISO 3166			

Table 21 – State Line Crossing Message Details



3.4.3 J1587 for Current State and Country– Only on “Low-Speed” Networks with Sophisticated GPS and On-Board Databases or External Communications

This specialized message could be available in some vehicles and would provide the state and country when demanded. This does not represent all the required data but could save some processing. Table 22 below shows the results.

Measure	Byte Pos	Value From	Encoding	J1587 Ref
Current State	1-3	Postal Code 65	3 Char Max for each	A.219
Current Country	4-6	ISO 3166		Page 126

Table 22 – State Line Crossing Message Details

3.4.4 J1587 for Milepost ID – Only on “Low-Speed” Networks

This specialized message could be available in some vehicles and could provide the latest milepost passed when demanded (limited to trucks with the sensor traveling on roads with the marked mileposts). This does not represent all the required data but could save some processing. Table 22 below has the results.

Measure	Byte Pos	Value From	Encoding	J1587 Ref
Milepost ID	1-4	Varies by sensor feed	4 Char Max	A.509 Page 186

Table 22 – Milepost ID Message Details

3.5 J1787 and J1939 Messages to Augment and/or Check Pre-Loaded Data

During the research for this document both the “low-speed” and “high-speed” networks yielded messages that could be used to check or augment the pre-loaded data – but only if the vehicles are equipped to support these messages. This would provide a check against the pre-loaded data. Messages for the vehicle VIN as well as Driver ID and Card Inputs could be utilized and the following sections provide the details.

3.5.1 J1587 or J1939-71 for the Truck VIN –Pre-Load or Tractor Swap Check

Both network types can provide the Vehicle Identification Number (VIN) if so equipped. This would provide a check against the pre-loaded data as well as a way to indicate that a Tractor was swapped out for Maintenance, etc. during a trip. Both network types return alphanumeric strings conforming to the ASCII Extended character set. The “high-speed” message is limited to 200 characters. Table 23 below shows the results.

Measure	#Bytes	Encoding	J1587 or J1939 Ref
VIN	As Req	ASCII Ext CharSet	J1587-A.239 - Page 135
VIN	200 Max		J1939-71/5.2.5.085 – Pg 290

Table 23 – Road Speed Measurement Message Details



3.5.2 J1587 or J1939-71 for Driver IDs –Preloads Verification

Both network types can provide text information about the driver(s). This could provide a check against the pre-loaded data. Both network types return alphanumeric strings conforming to the ASCII Extended character set with the asterisk “*” character as the delimiter between the Primary and Backup Diver. Table 24 below shows the results.

Measure	#Bytes	Delimiter	Encoding	J1587 or J1939 Ref
Driver 1 ID Data	As Req	“*”	ASCII Ext CharSet	J1587-A.507 - Page 185
Driver 2 ID Data	As Req			J1939-71/5.2.5.287 – Pg 338 J1939-71/5.3.145 – Pg 429

Table 24 – Driver ID Message Details

3.5.3 J1939-71 for Driver Card– Could verify Preloads and Status Changes

The J1939 has a PGN for Tachographs that returns an 8 Byte message with numerous datums. The 5th and 6th bit of the second and third bytes of this message indicates whether the drivers have their tachograph cards in place or not. The four possible responses are shown in Table 25 below.

PGN	Byte	Bit 5	Bit 6	Indicates	J1939-71 Ref
TCO1	2	0	0	Driver 1 Card Out	5.2.6.080 – Pg 237 5.3.143 – Pg 428
	2	0	1	Driver 1 Card In	
	3	0	0	Driver 2 Card Out	
	3	0	1	Driver 2 Card In	

Table 25 – Driver(s) Tachograph Cards In or Out Message Details

3.6 J1939-71 Messages to Detect Clock Tampering

The J1939-71 “high-speed” network provides six messages, all grouped under a single PGN, which indicates if one of the Date-time parameters has been changed. This could be used as a simple flag to indicate tampering, for example, when a status change or state border crossing event is initiated for HOS record generation. This would be evident as the system clock in the truck should not normally be changed during a trip by the driver. This is not affected by hourly offsets that a driver might input to the clock as time zones change – for which there are separate messages.



3.6.1 J1939-71 Indicates a Changed Clock Parameter

The six parameters can be changes across their entire range to allow the date and time to be set as needed. For HOS compliance reviews, it is important to check if any change to the new and old value has occurred. Although difficult to indicate any real-time tampering, downstream processing of the trip records could indicate questionable patterns of clock changes. Table 26 shows the 6 possible adjustments.

Measure	Range	Resolution	Encoding	J1587 Ref
Adjust Seconds	0 to 59.75	.25	US Short Int	5.2.5.288 – Pg 338
Adjust Minutes	0 to 59	1	US Short Int	5.2.5.289 – Pg 338
Adjust Hours	0 to 23	1	US Short Int	5.2.5.290 – Pg 338
Adjust Month	1 to 12	1	US Short Int	5.2.5.291 – Pg 338
Adjust Day	.25 to 31.75	.25	US Short Int	5.2.5.292 – Pg 339
Adjust Year	1985 to 2235	1	US Short Int	5.2.5.293 – Pg 339

Table 26 – Road Speed Measurement Message Details

3.7 J1939-71 Messages to Directly Recover Duty Status Changes

There are messages in the J1939 “high-speed” network that basically map to the Duty Status Codes. In trucks with automated tachographs these status indicators can be discretely demanded. In trucks with this feature and an integrated GPS system the HOS process could be almost if not completely automated. The next section shows the status message and the mapping to the HOS duty status codes.

3.7.1 J1939-71 Bit States Showing Driver Status

The J1939 has a PGN for tachographs that returns an 8 byte message with numerous datums. Bits 1 to 6 of the first byte of this message can be mapped to HOS Duty Status Change Codes. The ten possible responses (five for each driver) are shown in Table 27 below.

PGN	Measures	Dvr	Byte	Bit1	Bit2	Bit3	Maps to HOS	J1939-71 Ref
TCO1	Rest	1	1	0	0	0	Sleeper Berth	5.2.6.077 Page 361
	Short Break	1	1	0	0	1	Off Duty	
	Loading	1	1	0	0	0	On Duty - Not Driving	
	Driving	1	1	0	0	1	On Duty - Driving	
	Not Avail	1	1	1	1	1	Off Duty	
	Measures	Dvr	Byte	Bit4	Bit5	Bit6	Maps to HOS	5.3.143 Page 428
	Rest	2	1	0	0	0	Sleeper Berth	
	Short Break	2	1	0	0	1	Off Duty	
	Loading	2	1	0	0	0	On Duty - Not Driving	
	Driving	2	1	0	0	1	On Duty - Driving	
Not Avail	2	1	1	1	1	Off Duty		

Table 27 – Driver(s) Tachograph Cards In or Out Message Details



ECM and TCM Usage for HOS Solutions

SECTION 4 – RECOMMENDATIONS

The recommendations covered in the body of this document are compiled here resulting in a table that indicates the recommended network messages that could be used in HOS solutions.

The report's important recommendation is that any **HOS solutions should use demanded data from both the "low-speed" J1587 and "high-speed" J1939-71 messages.**

HOS solutions should demand location data from GPS systems residing on vehicle networks first and get location data via a direct connection to the GPS receiver as a second and/or backup option. Data passed directly through the vehicle network can provide the latitude and longitude to the HOS solution discretely. This data can also be loaded, after interim calculations, from the GPS unit directly. Demanding the data from an integrated GPS system will provide the data with less associated computing and provide better performance in the HOS solution.

The "low-speed" J1587 messages for State Line Crossings (A.218) and Current State and Country (A.219) should not be used for HOS Solutions. These messages could provide partial data to slightly lessen the driver inputs during Status Change and State Border Crossing events but could be automated by direct GPS inputs. For the "low-speed" network to compute the State Line Crossing and Current State and Country message contents they would use latitude and longitude data, which can be used directly by the HOS solution to do same thing but provide the complete HOS data needed for the compliance record.

The "low-speed" J1587 Mile Post Identification (A.509) messages should not be used for HOS Solutions. The Mile Post Identification record can only be provided by vehicles with the sensor installed while driving on roads whose mile posts have been modified to provide the information. In our opinion, this would not represent a significant percentage of the HOS records that would be gathered thereby making the incorporation of this message non cost-effective for HOS solutions.

HOS solutions could use the J1939-71 Tachograph messages for better solution automation. The J1939 Tachograph PGN offers message content that can help automation. When the HOS Software Design Spec is undertaken, poll industry to gauge the number of new vehicles being produced with integrated GPS and Tachograph systems which could completely automate HOS data gathering with a dedicated firmware solution as a J1939 network node. If the industry poll indicates these integrated GPS and Tachograph systems make up a significant portion of the fleet or are trending to do so, then add another class to the Software Design Specification to describe the fully automated solution.

In general, **all vehicle network messages used to provide HOS data should use the highest Priority Messages as their primary source for information.** This will minimize data access times and maximize HOS solution performance.



ECM and TCM Usage for HOS Solutions

The following messages shown below in Table 28 should be used to address the HOS Data Items required for Part 395 Compliance.

#	Rationale	Type	Description	Low Speed J1587		High Speed J1939-71				
				Para	Page	SPN	Para	Page		
1	§395.15(c)(1)	I	Status - Off Duty			1612	5.2.1.012	237		
2	§395.15(c)(2)	I	Status- Sleeper Berth			1613	5.2.1.012	237		
3	§395.15(c)(3)	I	Status- On Duty - Not Driving			1615	5.2.6.080	362		
4	§395.15(c)(4)	I	Status- On Duty - Driving			1616	5.2.6.080	362		
5	§395.15(c)(5)	D	Date-Time Group	A.251	140	959	5.2.5.093	292		
				A.252	141	960	5.2.5.094	292		
				A.253	141	961	5.2.5.110	297		
						962	5.2.5.111	297		
						963	5.2.5.112	297		
				964	5.2.5.113	298				
6	§395.15(c)(6)	C	Total Miles Driving Today	A.245	138	245	5.2.5.051	283		
7	§395.15(c)(7)	P	Truck/Tractor & Trailer Number	A.237	134	237	5.2.5.087	291		
8	§395.15(c)(8)	P	Name of Carrier							
9	§395.15(c)(9)	P	Main Office Address							
10	§395.15(c)(10)	P	24-hour period starting time							
11	§395.15(c)(11)	P	Name of Co-Driver	A.447	172	1626	5.2.5.287	338		
				A.507	185					
12	§395.15(c)(12)	C	Total Hours	A.245	138	245	5.2.5.051	283		
				A.251	140	959	5.2.5.093	292		
				A.252	141	960	5.2.5.094	292		
						961	5.2.5.110	297		
						962	5.2.5.111	297		
				963	5.2.5.112	297				
				964	5.2.5.113	298				
13	§395.15(c)(13)	P	Shipping Doc Numbers, etc.							
14,15	§395.15(d)(1,2)	D,I	Location as numeric code	A.239	135	584	5.2.5.086	290		
						585	5.2.5.087	290		
16	Data Security	P	Driver Identification	A.447	172	1625	5.2.5.287	338		
			A.507	185						
17	Safety Issue	C	Truck is <u>Moving</u> or <u>Not Moving</u>	A.84	71	84	5.2.5.012	237		
						A.160	99	160	5.2.5.054	284
								516	5.2.1.011	237
								1611	5.2.6.078	361
18	Tampering	C	Date-Time Group was Adjusted			1603	5.2.5.288	338		
						1604	5.2.5.289	338		
						1605	5.2.5.290	338		
						1606	5.2.5.291	338		
						1607	5.2.5.292	339		
						1608	5.2.5.293	339		

Table 28 – Recommended ECM Messages for HOS Data Items



ECM and TCM Usage for HOS Solutions

Finally, HOS solutions should exploit the large array of Commercially Available Hardware to convert the RS-485 or J1939 network protocols to a more widely-used standard like the RS-232 Serial Specification. This will provide an open hardware interface for HOS solutions.



BIBLIOGRAPHY

The documents used in the research for this module are listed below. The CD ROM delivered with this report contains files in Portable Document Format (PDF) and standard graphics. The only documents excepted are the SAE Documents that require subscription.

#	Type	Title
1	Standard	SAE J1708 – Serial Data Communications Between Microcomputer Systems in Heavy Duty Vehicle Applications
2	Standard	SAE J1587 - Electronic Data Interchange Between Microcomputer Systems in Heavy-Duty Vehicle Applications
3	Standard	SAE J1939 – Truck and Bus Control and Communications Network Standards Manual
4	Paper	AVT Inc. - In-Vehicle Computer Networks - An Overview
5	Paper	B&B Electronics – The Basics of the RS-485 Standard
6	Paper	Transportation Research Board – AVL Systems for Bus Transit (TRCP24)
7	Paper	ITE – ITS Standards Outreach Work Plan
8	Graphic	IXXAT Automation – CAN Basic Timing Signal Schema
9	Graphic	IXXAT Automation – CAN Data Frame Schema
10	Paper	IXXAT Automation – CAN-based Higher Layer Protocols and Profiles (Paper)
11	Paper	IXXAT Automation – Controller Area Network - Introduction
12	Paper	IXXAT Automation – DeviceNet - Introduction
13	Paper	IXXAT Automation – CAN-based Higher Layer Protocols and Profiles (Web)
14	Paper	SAE (CiA) - Gateway Between CANopen and ISO 11992 or SAE J1939
15	Paper	SAE (Delphi) - Mobile Multi Media Open Computing Platform
16	Paper	iCC 1995 (SAE) - Implementation of CAN for Heavy Duty Truck and Bus Market -- Specification J1939
17	Paper	TMC – Future Driver Interface
18	Paper	TMC – Innovation in Future Truck Cab Designs
19	Paper	TMC - Future Cab Study
20	Paper	TMC – Tomorrow’s Truck Committee Position Paper Series
21	Paper	Unknown – Standards Development Plan
22	Article	ATA - Black Boxes, Satellites & Safety: Q&A
23	Article	ATA - ATA To FHWA: Involve Truckers, Protect Data In ITS Planning
24	Article	ATA - NTSB Likely To Recommend ‘Black Boxes’ On All Highway Vehicles
25	Article	AVT Inc. - Controller Area Network {CAN}
26	Article	EnGenius - VXIBus Mezzanine Modules Maximize I/O and Function Choices
27	Catalog	Apex Industries - Pro-Link Diagnostic Scan Tools



ECM and TCM Usage for HOS Solutions

#	Type	Title
28	Hardware	AVT Inc. – Model 512 M-Module Interface Press Release
29	Hardware	AVT Inc. – Model 512 M-Module Interface Specification
30	Hardware	AVT Inc. – Model 717 UBP and CAN Interface Specification
31	Hardware	AVT Inc. – Model 718 Multiple Interface for Auto Networks Press Release
32	Hardware	AVT Inc. – Model 718 Multiple Interface for Auto Networks Specification
33	Hardware	Cummins – QuickCheck II PDA-based Scanning Tool
34	Hardware	Delphi – ETC 2.2 Heavy Duty Diesel Controller
35	Hardware	EnGenius - MultiCom III/s Multi-Purpose Vehicle Interface
36	Hardware	EnGenius - MultiCom II Multi-Purpose Vehicle Interface (ISA Card)
37	Hardware	MagiKey – Parallel Port Data Module – P/N 126032
38	Hardware	VIA - RS-232 to J1708 Converter – P/N J1708D15
39	Software	AccuTest - CANalyzer Win Analysis Software
40	Software	Microsoft – Data Type Summary (from MSDN)
41	Software	Microsoft - IEEE Standard 754 Floating Point Numbers
42	Software	Noregon Systems – JPRO TM J1708 RP1210A-Compliant API
43	Software	DG - HERCULES CAN Analysis Software Overview
44	Software	DG – High Resolution HERCULES Software Screen Shot
45	Software	DG - HURCULES CAN Analysis Software Users Manual



**Federal Motor Carrier Safety
Administration**

Office of Business and Truck Standards and Operations

**Research and Analysis on Using
Geo-Referenced Data in
Hours of Service Solutions**

January 21, 2003



ECM and TCM Usage for HOS Solutions

TABLE OF CONTENTS

Section Page
TABLE OF CONTENTS II
SECTION 1 - EXECUTIVE SUMMARY 3
SECTION 2 - RELEVANT PUBLIC DOMAIN DATA SOURCES 4
2.1 Public Domain Place Name Data Sources 4
2.1.1 USGS Geographical Names Information System (GNIS) 4
2.1.2 FIPS 55-3 Codes for Named Populated Places 5
2.1.3 "U.S. Gazetteer 2000" Data from the Census Bureau 5
2.2 Public Domain State Border Crossing Data Sources 7
2.2.1 USGS 1:24,000 "Quad" Map Digital Data 7
2.2.2 USGS 1:100,000 "Quad" Map Digital Data 7
2.2.3 USGS 1:2,000,000 Digital Line Graph Data 7
SECTION 3 - DATA CONSOLIDATION ISSUES 10
3.1 Cartography Basics 10
3.1.1 The WGS 84 Baseline Ellipse 11
3.1.2 Projection Basics 11
3.1.3 The Lambert Conformal Conic Projection 13
3.1.4 Recommended HOS Coordinate Grid 14
3.2 Recommended Place Name Data Set for HOS Solutions 15
3.2.1 Small Communities in Large Cities Using City Circles 15
3.2.2 Dataset Reduction Using Cutoff Population Filters 19
3.2.3 Place Name Analysis Utility 20
3.3 Recommended State Border Crossing Data Set for HOS Solutions 22
3.3.1 Baseline Data Condenser Utility 23
3.3.2 State Border Crossing Matching Utility 24
3.3.3 Removing Duplicate Matches 24
3.3.4 Adding International SBC Records 25
3.3.5 Final Checks and Recommended SBC Dataset 25
SECTION 4 - PLACE NAMES AND STATE BORDER CROSSING DATA IN HOS SOLUTIONS 27
4.1 Front End Solutions 27
4.2 PC-Based Back-End Portable CPU Solutions 28
SECTION 5 - RECOMMENDATIONS 29
BIBLIOGRAPHY 31



SECTION 1 – EXECUTIVE SUMMARY

FMC Regulation Part 395 requires location information when a change in Driver Status or State Border Crossing occurs. The name of the nearest named place or road(s) that cross the border is required. HOS solutions with on-board GPS systems will be able to store the demanded Latitude and Longitude in the HOS record and additional data could be incorporated into the solutions to recover a numeric code that would also be stored.

HOS solutions with no GPS system will not be able to provide the Latitude and Longitude but will still need the numeric code. Therefore, additional data will be required in these solutions to allow the Driver to efficiently look-up the numeric code based on a hierarchical scheme, starting with the State, then the City or Metropolitan Area for a Place Name; or States on either side of a border, and the road the vehicle is crossing on for State Border Crossings.

To recommend specific data for the Place Name information a number of public-domain data sources were reviewed. The Census Bureau's "U.S. Gazetteer 2000" data is recommended for Place Names and would be used that provides the nearest City or Metropolitan Area when the Driver Status changes. That list contains 25,375 place names, a significant number of which can be eliminated without adversely affecting the applicability of the data.

Data filtering, using a cutoff for the total population effectively eliminated un-needed Place Names. Also, the use of a circular area to eliminate small communities from large cities (city circles) for better data context further reduced the total to 6,962. The baseline list with 25,375 Place Names and the list with the recommended 6,962 Place Names for HOS solutions are included on the attached CD in references 6 and 9 respectively.

To recommend specific data for the State Border Crossing information, more public-domain sources were reviewed. The United States Geological Survey (USGS) Digital Line Graph data at 1:2,000,000 data was used. This data, on a state by state basis, provides multi-segment line data for both roads and state boundaries.

Custom software was developed and used to isolate the State Border Crossing points between the Lower 48 states. Crossings at International borders were added manually. This resulted in the recommended list of 2,350 State Border Crossing points. This recommended list is included on the attached CD in reference 14.



ECM and TCM Usage for HOS Solutions

SECTION 2 - RELEVANT PUBLIC DOMAIN DATA SOURCES

Any future HOS solution requires the nearest “place name” to be included in each data record. The place name is simply the nearest town, city, village, etc. that will indicate where the vehicle was when the HOS record was recorded. There is also a requirement to record the mileage traveled in each State. This requires a State Border Crossing event to be recorded when a state border is crossed. In both cases this includes the vehicles’ location, and geographical reference (or geo-referenced) coordinates to calculate the nearest Place Name. The miles traveled in the State would be computed as the difference between the collected odometer readings.

Two distinct groups of information are required, first is the vehicle position and second is a software module in the HOS solution that recovers the nearest place name (PN) or state border crossing (SBC) based on the first group. Since not all vehicles will have an on-board Global Positioning Satellite (GPS) System, the first group of information could also be obtained from direct input from the driver.

If there is a GPS on-board, the vehicle’s position is assumed to be provided numerically as the Latitude and Longitude for that point on the Earth’s surface. This will explicitly define the position of the vehicle. If there is no GPS system, the driver will have to input information about “where” the vehicle is to have the second software module mentioned earlier recover the nearest PN or SBC.

In any event, the software will contain a database that provides the PN and SBC data based on inputs from the GPS or driver. This will enable vehicles with GPS to provide coordinates to be used to extract the appropriate PN or SBC for the HOS record. This data source could allow the driver to obtain the PN or SBC in a “top-down” fashion when there is no on-board GPS.

Without GPS the driver would probably first input the state and then look up the city, town, etc. There are 3 public domain sources for place name data and 3 for state border crossing data. These are described in the succeeding sections of the document.

2.1 Public Domain Place Name Data Sources

2.1.1 USGS Geographical Names Information System (GNIS)

The United States Geological Survey (USGS) maintains detailed source information called the Geographical Names Information System (GNIS) which is available “on-line” for the conterminous (lower 48) states. The current list of place name record is included in the attached CD that delivers this document as a text file and contains over 200,000 records. Implementing this large number of records in any HOS solution would result in too detailed a location archived in HOS records. Although the vehicle’s location would be described in great detail, the context might not be optimal for those who would review it.

GNIS data does not provide consistent measures (population and other demographics) that would allow the large number of records to be filtered such as the population of the Place Name. So while the GNIS data could be used in HOS solutions there is no easy way to filter this data to make it effective for use in vehicle software. In short, GNIS does not adequately support a HOS Solution.



ECM and TCM Usage for HOS Solutions

2.1.2 FIPS 55-3 Codes for Named Populated Places

The Federal Information Processing System (FIPS) is a group of data and standards documents that provide information about a wide variety of Information Technology (IT) areas. The FIPS 55-3, maintained by the National Institute of Standards (NIST) contains information about “Named Populated Places”. This data is contained in 132 character records with the named place and numeric codes (useful for efficient HOS data records) – but no Latitude and Longitude.

This lack of latitude-longitude coordinates also makes the FIPS 55-3 data less than user-friendly for HOS solutions. To mask this problem, software could be devised to map the GNIS and FIPS 55-3 data together, using the Place Name as the common datum, which would result in a combined set with the necessary data points. However, even if that were accomplished the combined data would still not contain the optimum data for filtering the large number of fields.

What is required is a dataset that has the Latitude and Longitude coordinates and the numeric codes for the Place Names, as well as some method of filtering for population, land area, etc. The next section depicts a public domain dataset that does this.

2.1.3 “U.S. Gazetteer 2000” Data from the Census Bureau

The Bureau of the Census (BoC) collects generalized demographic data during the 10-year National Census activities. Among the many data products that result from this is the “U.S. Gazetteer” data which has the location, place name, and filtering data in a single source. **We recommend that the “U.S. Gazetteer 2000” (current information derived from the 2000 Census) data set be used for HOS solutions.**

Data is included for all 50 states, the District of Columbia, and Puerto Rico and is available “on-line” in four distinct datasets. They are:

- Places – Contains 25,375 records for place names and is the data applicable to HOS solutions. 225 of the records are for Puerto Rico and are not applicable to this analysis.

The other three are not of direct interest to HOS and include:

- Counties – Contains 3,219 records
- County Subdivisions – Contains 36,351 records
- ZIP Code Tabulation Areas (ZCTAs)– Contains 33,233 records

This analysis recommends that the BoC U.S. Gazetteer 2000 (G2000) data be used for HOS solutions. This research examined the 32,375 baseline record for direct usage in HOS solutions. While it is possible to handle all the records in a single software module the context problem with the large 250,000+ GNIS records is also present in the 32,375 G2000 data set. This context problem has two types, at either end of the population spectrum.

The first is handling small communities in large cities. The G2000 data can provide very definitive locations which will not have good context to a downstream HOS records reviewer. It is better to filter out the small communities within large cities to eliminate this. The Latitude and Longitude (obtained directly from a GPS system or from a Place Name lookup via driver input)



ECM and TCM Usage for HOS Solutions

is stored in the record. If an exact location is desired in a GPS-capable systems, a “back-end” system utility could be used.

The second context problem is handling Place Names with very small populations. A disadvantage of using the BoC data is that very small places make up a large proportion of the database: 22½% of the 32,375 records (almost 7,300) indicate 2000 Census populations of 500 or less (18 show a zero population). The vast majority of these are not likely to provide good context for HOS solutions.

A custom software application was developed to study and validate the optimum place name data set and is documented in Section 3.4 of this document. The Places file contains 32,375 records, each 164 characters long, which contain the data. Table 1, shown below, provides the Metadata for the U.S. Gazetteer 2000 file.

#	Column Range	Metadata	HOS Data Record Usage
1	1-2	United States Postal Service (USPS) State Abbreviation (Postal Code 65)	These are the numeric codes – this analysis recommends that they be mandated for HOS solutions to ease automation and enforce an approved standard
2	3-4	FIPS 55 State Code	
3	5-9	FIPS 55 Place Name Code	
4	10-73	Place Name	The place name itself
5	74-82	Total Population	These fields could be used for filtering purposes – this study concentrated on the population data in field 5
6	83-91	Total Housing Units	
7	92-105	Land Area (M ²)	
8	106-119	Water Area (M ²)	
9	120-131	Land Area (mi ²)	
10	132-143	Water Area (mi ²)	
11	144-153	Latitude (DD) - First character is blank (N) or "-" (S) - For the U.S. this should always be positive (Northern Hemisphere)	Latitude and Longitude for lookup against GPS input (On-Board GPS)
12	154-164	Longitude (DD) - First character is blank (E) or "-" (W) - For the U.S. these will always be negative	Direct storage when driver identifies the Place Name directly (No on-board GPS)

Table 1 – BoC “U.S. Gazetteer 2000” Metadata

The first three fields provide all the USPS and FIPS codes that would be directly stored in the HOS records with the correlating Place Name in Field 4. Data for filtering the number of place names stored in an HOS solution could be filtered by the data related in fields 5 to 10. Lastly, the Latitude and Longitude are directly available, converted to decimal degrees, for the location. The precision of the Latitude and Longitude are more than adequate for the needs of the HOS solution, providing positions equivalent to the positions derived from an on-board GPS system.



ECM and TCM Usage for HOS Solutions

2.2 Public Domain State Border Crossing Data Sources

2.2.1 USGS 1:24,000 "Quad" Map Digital Data

The United States Geological Survey (USGS) has created and maintained an excellent source of quadrangle or "quad" maps of all 50 states for decades. These maps cover $7\frac{1}{2}$ degrees of arc or about 8.65 miles on a side. More recently these maps have been digitized and can be interrogated using automated techniques.

There are files for each "quad" map that contain data for both roads and state lines – the intersections are of HOS interest. However, they do not lend themselves directly to automated searches as the edges of the data are trimmed along discrete values for Latitude and Longitude. This process does not correlate with the roads and state border elements of interest.

Maps are required that are with the edges digitally trimmed at the state borders, making it easier to search for the roads that cross. Both the less detailed 1:100,000 and 1:2,000,000 million data sets are organized this way and are described in the next two sections.

2.2.2 USGS 1:100,000 "Quad" Map Digital Data

The USGS also maintains the 1:100,000 scale Digital Line Graph (DLG) data that are derived from USGS 1:100,000-scale, 30- by 60-minute quadrangle maps. Like the 1:24,000 scale maps there are entities data for roads and state boundaries but the level of detail is finer than we would recommend for HOS solutions.

Commercial motor vehicles (CMVs) frequently use limited access, federal, and state roads when crossing border crossings. The 1:2,000,000 scale maps offer a better source for the HOS data and are described in detail in the next section.

2.2.3 USGS 1:2,000,000 Digital Line Graph Data

The USGS also offers the 1:2,000,000 scale DLG data which is organized by State. They contain information on layers to include transportation, hydrography, and boundaries for all 50 States.

Of interest for the HOS solutions are the maps based on States as the data is trimmed to borders. These are ideal for the HOS problem as the lines plotted out in the graphs have multiple segments, forming open ended polygons, called polylines. The ends of these polylines for roads and borders can be compared, yielding the discrete border crossings directly.



ECM and TCM Usage for HOS Solutions

The following is an example of data as plotted from above, as well as the Hydrography type (not used for HOS), and is the input in computing the border crossings. The following lines show an example for the Transportation data type in Virginia.

```
DESCRIPTION=SECONDARY ROUTE, CLASS 2, SYMBOL UNDIVIDED
NAME=US17
ENTITY_LABEL=1700205
ROUTE_NUMBER=US17
ROUTE_NUMBER=US50
-78.090523,39.079346,0.0
-78.104624,39.085851,0.0
-78.114639,39.089136,0.0
-78.120368,39.099626,0.0
-78.124733,39.119620,0.0
-78.129254,39.131456,0.0
-78.136768,39.141964,0.0
-78.150259,39.150271,0.0
```

```
DESCRIPTION=PRIMARY ROUTE, CLASS 1, SYMBOL UNDIVIDED
NAME=I 81
ENTITY_LABEL=1700201
ROUTE_NUMBER=I 81
-78.181633,39.121596,0.0
-78.190115,39.111713,0.0
-78.196263,39.099539,0.0
-78.200047,39.086886,0.0
-78.202596,39.076940,0.0
```

The leading lines of the record describe the route type and provide the name(s) for the route. This is of interest for the State Border Crossings as the <ROUTE_NUMBER> indicates whether more than one designation is used for that polylines. Note that the first record is a polyline representing both US 17 and US 50 whereas the second record is just for I 81.

The triple set of numbers that follow shows the angular measures for the polylines with Longitude first, then Latitude; the third parameter is not used. For HOS purposes only the first and last points of the polylines (for Roads) are needed as one end or the other could end at the state line Boundaries and needs checking.

Regardless of whether Place Name or State Border Crossing is desired, the Latitude/Longitude angular measures have to be converted to XY coordinates using a map projection. The figure above uses the Lambert Conformal Conic projection which is commonly used for the 48 Conterminous States

Section 3 of this document discusses the basics of Cartography and Map Projections and their application to HOS solutions.

SECTION 3 –DATA CONSOLIDATION ISSUES

The recommended BoC G2000 data for place names needs to apply effective techniques for filtering the 32,375 records to a smaller number of records that will provide better context in HOS solutions. Part 395 requires that the distance to and name of the nearest place be related in the HOS records when a driver status change occurs.

This distance lies along the surface of the earth and has units of length (miles, kilometers, etc.) not the decimal degrees used for the angular measures of Latitude and Longitude. To convert the Latitude and Longitude to Cartesian (or X,Y) coordinates we will use a Map Projection so that the distance can be easily computed using the Pythagorean Theorem. The next section gives a brief overview of Cartography with a recommended Projection for use in HOS computations.

3.1 Cartography Basics

HOS solutions need to identify the location of points on the Earth based on the latitude and longitude data provided by the G2000 data. Latitude and longitudes are measured in the earth's graticule which is the network of latitude and longitude lines superimposed on the surface the earth.

Latitudes are also commonly referred to as Parallels and Longitudes are as Meridians. The Parallels of Latitude are formed by E-W circles surrounding the Earth in planes "parallel" to the Equator. The latitude angle ranges from -90 deg (sometimes shown as 90 deg South) at the South Pole to +90 deg (sometimes shown as 90 deg North) at the North Pole. Figure 2 at the right, depicts the earth's graticule.

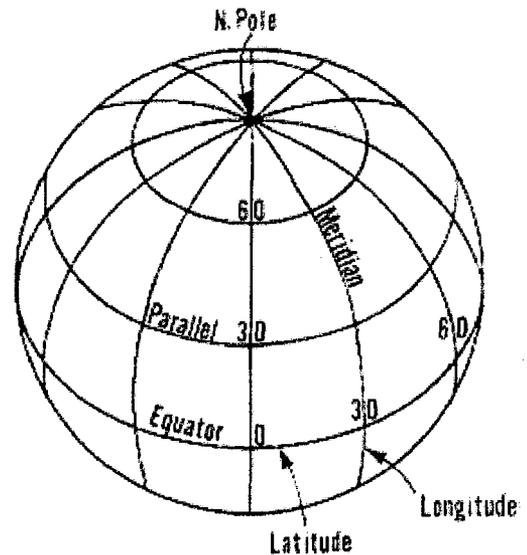


Figure 2 – The Earth's Graticule

Meridians of longitude are formed with a series of N-S lines, all intersecting at the Poles. The Parallels and Meridians cross each other at 90 degrees to each other. The Longitude angle ranges from -180 deg (sometimes shown as -180 deg West) to +180 deg (sometimes shown as 180 deg East). The zero Meridian was historically set at Greenwich, England, making all of the United States Longitude values negative. Likewise the United States lies in the Northern Hemisphere making the Latitude values all positive.

While the length on the surface of a degree of Latitude is always the same on a sphere, the lengths of degrees of Longitude vary with the Latitude. Along the Equator the length of a degree of Latitude and Longitude are the same. To convert these angular measures requires a "Map Projection" which is a device for producing all or part of the earth's features in two dimensions.



ECM and TCM Usage for HOS Solutions

This cannot be done without some distortion. For HOS it is desirable to minimize this. Most projections are defined by choosing different points on the Earth as the center or as a starting point – this study will focus on the 48 Conterminous States, Alaska, and Hawaii as three separate entities for these projections.

3.1.1 The World Geodetic System 84 Baseline Ellipse

For many map projections the shape of the Earth is assumed as a sphere. In reality it is more nearly an oblate ellipsoid of revolution, also called an oblate spheroid which is an ellipse rotated about its shorter axis. The flattening of the ellipse for the Earth is only about one part in three hundred, which is unfortunately sufficient to introduce significant errors in the relatively small distances that the HOS solutions will compute.

The Earth is not an exact ellipsoid and as technology has allowed more accurate measurements of the ellipsoid model parameters the “baseline” numbers have changed slightly. The most widely used ellipse of the Earth in maps of the United States is the World Geodetic System (WGS) from 1984, commonly called the WGS 84 ellipse.

The two parameters used in the Map Projection are the radius at the Equator (6378137 Meters) and the amount of flattening at the Poles (about 1/3 of a percent). With this information determined the choice of an appropriate map projection is addressed in the next section.

3.1.2 Projection Basics

There are an infinite number of mathematical constructions that can be used to project the angular measures of Latitude and Longitude into a two-dimensional plane. There have been hundreds of projections published of which a dozen or so are currently used for most mapping applications. There are 3 basic characteristics of Map Projections to consider:

Area - Projections are generally designed to be equal-area which means that a circular shape on one part of the projected two-dimensional map covers exactly the same area on any other part of the map. To do this the shapes and scale of the map must be distorted. The best projection for a particular application minimizes these shape and scale distortions.

Shape - Many of the most common and most important projections are orthomorphic (commonly called conformal), meaning that the smaller the feature plotted the more accurate is it's location. This is what is needed for HOS place name locations. Conformal projections produce relative angles at each point that are correct, meaning that the scale in any direction is the same – again important for HOS as the vehicle's location is provided by the GPS and a distance to the nearest place name at an arbitrary azimuth angle is computed.

Scale – Projections never show the scale correctly throughout the map and the best projection for a particular application will provide a minimum variation in scale. For the Conterminous United States the best accuracy is 1-2%.



ECM and TCM Usage for HOS Solutions

There are also three developable surfaces of interest commonly used in map projections. These give an indication of how the spherical surface is “unfolded” to a plane of the map. The three shown below are typically used for the United States. They are the Cylindrical, Planar, and Conical projections. Figure 3 at the right shows the notion of the three developable surfaces imposed on a graticule.

Cylindrical - If a cylinder is wrapped around the graticule so that it's surface touches the Equator all the way around, the Longitudes may be projected onto the cylinder as equidistant. Latitudes around the circumference of the cylinder and become distorted vertically. As the Latitude approaches +/- 90 degrees they stretch away to infinity.

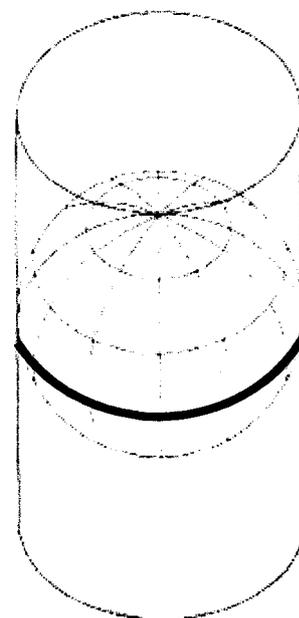
The most common use of the Cylindrical Projection is the Mercator projection which is the best-known example and is widely used for large-scale nautical charts. It has been in use for centuries, originating in nautical charts not needing accurate navigation close to the Poles.

Planar - A plane perpendicular to an azimuth from the Earth's center out is the basis for Planar projections. Longitudes are projected as straight lines radiating from a point and Latitudes are complete circles, centered on the intersecting point or circle between the azimuthal line and the plane.

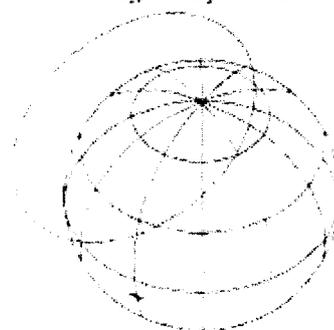
These projections are used more in specialized applications although the Oblique Stereographic Projection can be used for the United States with a 2% maximum error.

Conic - The best projection for HOS data is some form of a conic projection. If a cone is placed over the Earth's graticule with its central axis coincident with the Earth's rotational axis there will be a circular intersection at a Latitude (called a Standard Parallel). The Longitudes are projected as equidistant straight lines radiating from the apex of the cone, and the Latitudes are projected as lines around the circumference.

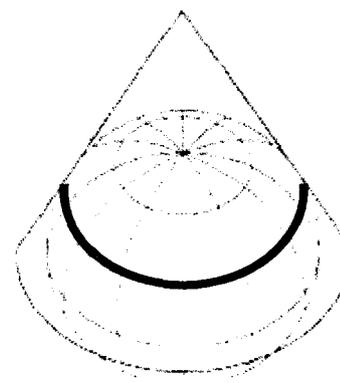
When the cone is cut along a meridian, unrolled, and laid flat, the meridians remain straight radiating lines, but the parallels are now circular arcs centered on the apex. If the cone is “lowered” toward the pole opposite the apex, 2 standard parallels results in better accuracy.



Regular Cylindrical



Oblique Azimuthal plane



Regular Conic

Figure 3 – The 3 Basic Projections



ECM and TCM Usage for HOS Solutions

This projection with 2 Standard Parallels is recommended for the HOS solutions. At each Standard Parallel the accuracy is perfect then being slightly under between them and slightly over above the northern standard parallel and below the southern standard parallel. Lambert proposed this projection in 1772 and it is still widely used today. It is called the Lambert Conformal Projection and is detailed in the next section.

3.1.3 The Lambert Conformal Conic Projection

The Lambert Conformal Conic projection was initially posed in 1772 and remained relatively obscure until World War I when it was used extensively by the French for their Military Maps of the day. Lambert developed the mathematics for both the Spherical and Ellipsoidal forms for two standard parallels which is what should be used for HOS solutions.

The Spherical and Ellipsoidal terms indicate that formulae can be used that model the Earth as a perfect sphere or (in our case) as the ellipse.

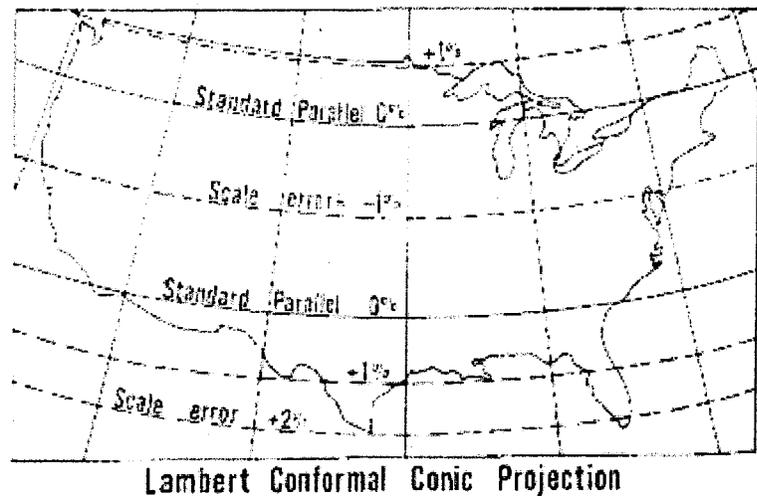


Figure 4 - Lambert Conformal Conic Mathematical Accuracy

Figure 4 above shows the relative accuracy for the Lower 48 States. Just along the Standard Parallels there is zero error. In between it is about -1% and above and below about +1%. The straight lines of Longitude represent lines drawn down the cone from its tip (or apex) to the circle around the bottom. South Texas and Central/South Florida will have between 1-2% errors. As the projection is extended toward the North Pole and/or Equator, the accuracy rapidly deteriorates.

The recommended Standard Parallels for this projection are 45 degN and 33 degN and were used for the calculations for both Place Name and State Border Crossings for the Lower 48, Alaska, and Hawaii. The Albers Equal Area Conic projection could also be used for the Lower 48 states but is not applicable for Alaska. We recommend the Lambert projection as its formulae can be used in HOS solutions for all areas of interest.

Once the WGS84 baseline ellipse, projection, and standard parallels are determined, only the Latitude and Longitude of Origin are needed to completely define the XY coordinate system (or grid) that will be used for the data conversion. This is described in the next section.

3.1.4 Recommended HOS Coordinate Grid

The use of a grid will allow X and Y coordinates, now distances instead of angles to define the points. The data that would be included in any HOS solution will have thousands of place names and state border crossing locations. Storing these as distances reduces the storage needed by 50%, which is important for firmware and low-end solutions that are storage capacity limited.

By choosing the appropriate units and origin location long integers (4 bytes each) instead of a double precision floating point (8 bytes each) can be used for data encodings. This analysis recommends that the origin for the Lower 48 states be taken at the lower left hand corner. This yields positive X, Y coordinates for the entire data set with distance units of meters fitting within the value range of a signed long integer. Figure 5 below shows an example of a map grid for the Lower 48 States with the State Boundaries and Interstate Highways plotted.

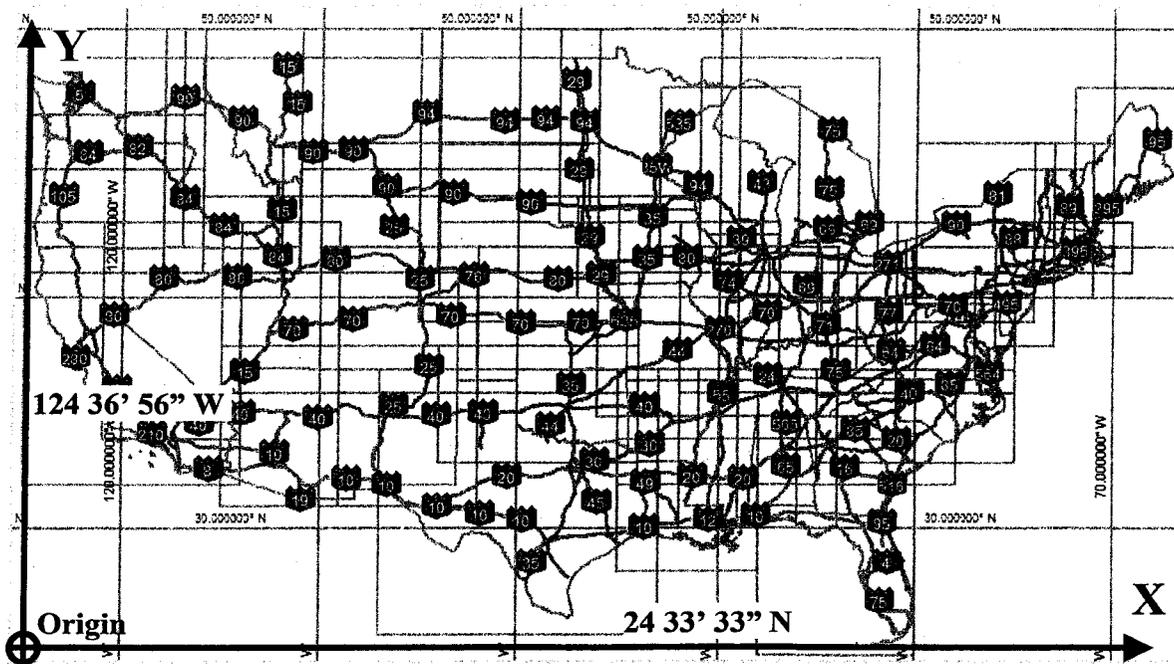


Figure 5 – Conterminous 48 States Grid

The origin was posed at the west-most Longitude of 124 degrees 36 minutes 56 seconds in western Washington State with the south-most Latitude of 24 degrees 33 minutes 33 seconds at the bottom of the Florida Keys. With the origin established and the projection and datum selected, any Latitude/Longitude pair can be converted to two integer values which are the meters east and north of this origin.

The same schema was posed for Alaska and Hawaii. Sections 3.2 and 3.3 that follow relate how the recommended PN and SBC datasets were derived using the projection described above.



ECM and TCM Usage for HOS Solutions

3.2 Recommended Place Name Data Set for HOS Solutions

The G2000 dataset with 32,375 records was used as the superset of Place Name (PN) information. Because many of these records will probably never be used as a location for a driver status change or state border crossing some filtering was accomplished to reduce the number of Place Names to be stored and used in HOS solutions.

The baseline PN data was not printed for direct inclusion in this document but is available in two forms on the attached CD. The first is a structured Excel spreadsheet that contains the baseline data as well as the formulae that applies the Lambert Conformal Conic projection to the angular data. It is the "2000 Census Place Names.xls" file at:

D:\Place Name Data\2000 Census Place Names\2000 Census Place Names.xls

The data without the projection information and the projection rationale only has been converted to PDF and is available on the attached CD in the Research Folder as "06 - Complete 2000 Census Place Names.pdf".

3.2.1 Small Communities in Large Cities Using City Circles

Large cities will usually have a proportional number of smaller communities interspersed within. Examination of the baseline G2000 data indicates that there are thousands of these sub-divisions included in the records. This raises the context problem mentioned earlier.

For example, a large city like Kansas City, MO contains dozens of small place names that should be filtered out. Adding to the complexity, because the metropolitan area straddles a state line, some will be in Missouri and some in Kansas. To give the filtered data good context we should set up CC's for Kansas City, MO and Kansas City, KS. This is done by establishing a circle at a point with a radius that eliminates the undesired Place Names.

This notion was applied across the Conterminous United States resulting in 138 individual City Circles applied to 129 cities. This is shown below at a high level of detail in Figure 7.

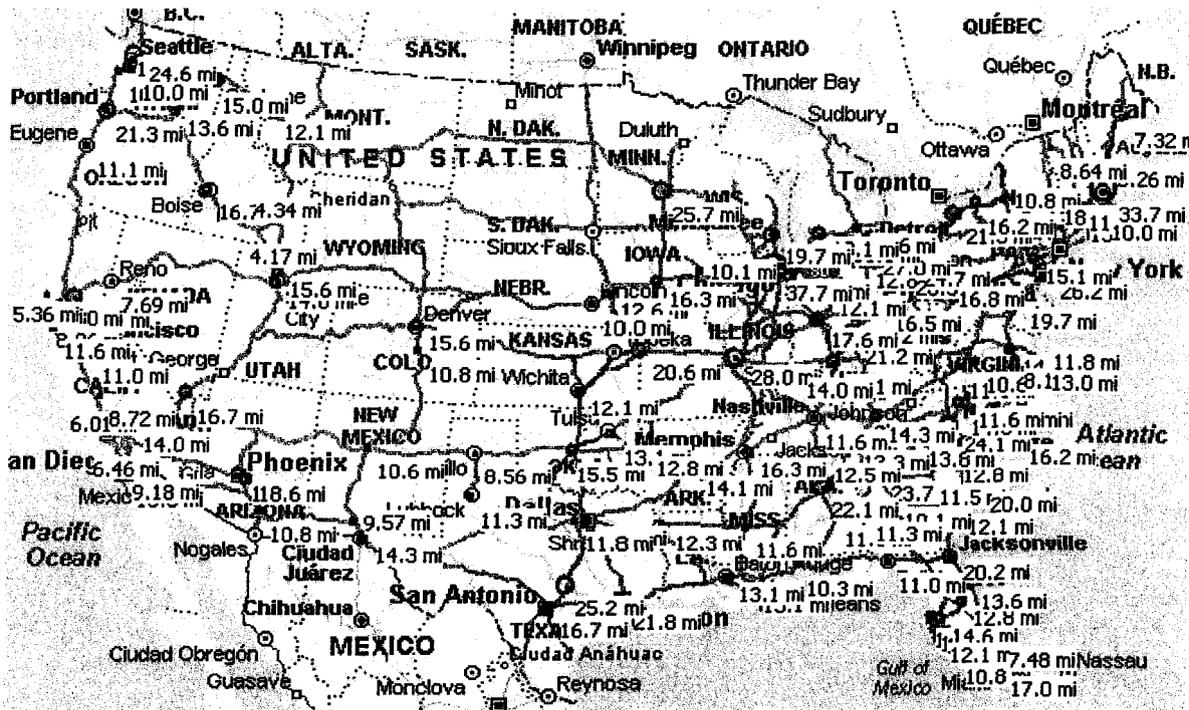


Figure 7 – City Circles Used for the Conterminous 48 States

The number of individual CC's and the cities they represent are not the same as because some cities require more than 1 CC to correctly capture the small communities within. Some cities, usually driven by their shape and/or proximity to another large city, will use more than 1 CC. A few metropolitan areas were assigned 2 CCs. One, San Diego, CA, was assigned 3 CCs.

A good example of this is the Virginia Beach/Norfolk/Hampton Roads area in southern Virginia. Norfolk and Virginia Beach are on the south side of the Hampton Roads estuary. Norfolk and Virginia Beach align themselves in an east-west axis with Hampton, VA to the north on the other side of the water.

An HOS record should differentiate between Hampton, VA and Virginia Beach, VA for status changes and a single circle for Norfolk and Virginia Beach cannot be posed without absorbing Hampton, VA.

To solve this problem two CCs are used for Virginia Beach/Norfolk and 1 Hampton. This way the small communities are condensed into the map correctly with good context for any HOS reviewer. South of the Hampton Roads the HOS record would indicate Norfolk/Virginia Beach and north of the Hampton Roads would indicate Hampton, VA.

This arrangement is shown below in Figure 8.

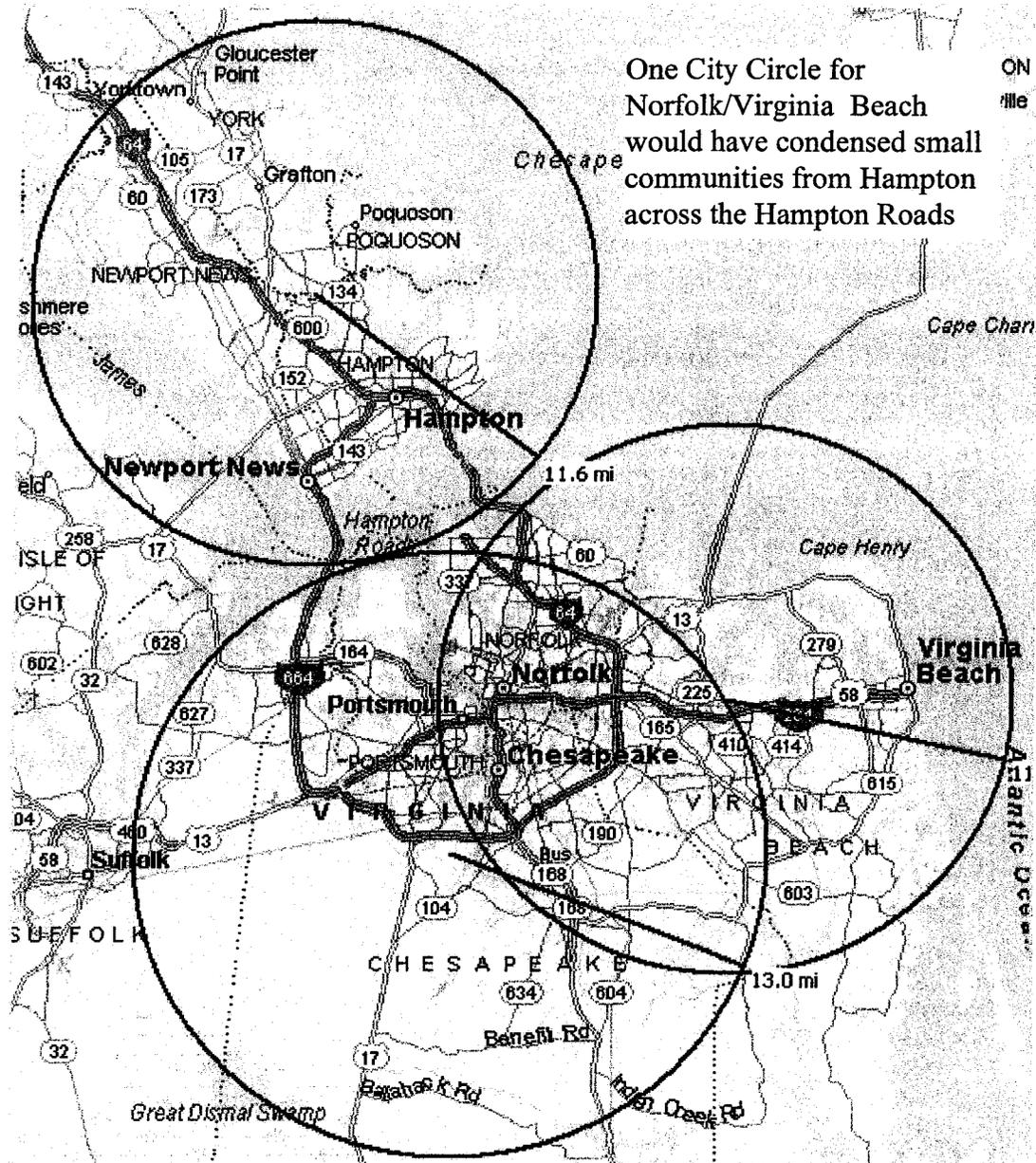


Figure 8 – City Circles Used for the Conterminous 48 States

The complete set of 139 City Circles were not printed for direct inclusion in this document but are available in two forms on the CD. The first is a structured Excel spreadsheet that contains the data as well as the formulae that applies the Lambert Conformal Conic projection to the angular measures. It is the “2000 Census Place Names.xls” file at:

D:\Place Name Data\2000 Census Place Names\2000 Census Place Names.xls



ECM and TCM Usage for HOS Solutions

The data without the projection information and the projection rationale only has been re-formatted for easier review and converted to PDF and is available in the Research Folder as "07 - Recommended City Circles for HOS Solutions.pdf". This data is used as input with the Place Name Analysis Utility that is described in section 3.2.3 to develop the recommended set of place names. City Circles were not applied for Alaska and Hawaii as these solutions could easily store the 339 and 131 records for Alaska and Hawaii respectively.

The next section discusses the use of a cutoff population filter that eliminates place names based on the indicated total population which is a field in the G2000 data (see Table 1).

3.2.2 Dataset Reduction Using Cutoff Population Filters

The baseline G2000 data contains 25,375 records. Figure 9 shown below depicts the distribution of total population across the entire dataset.

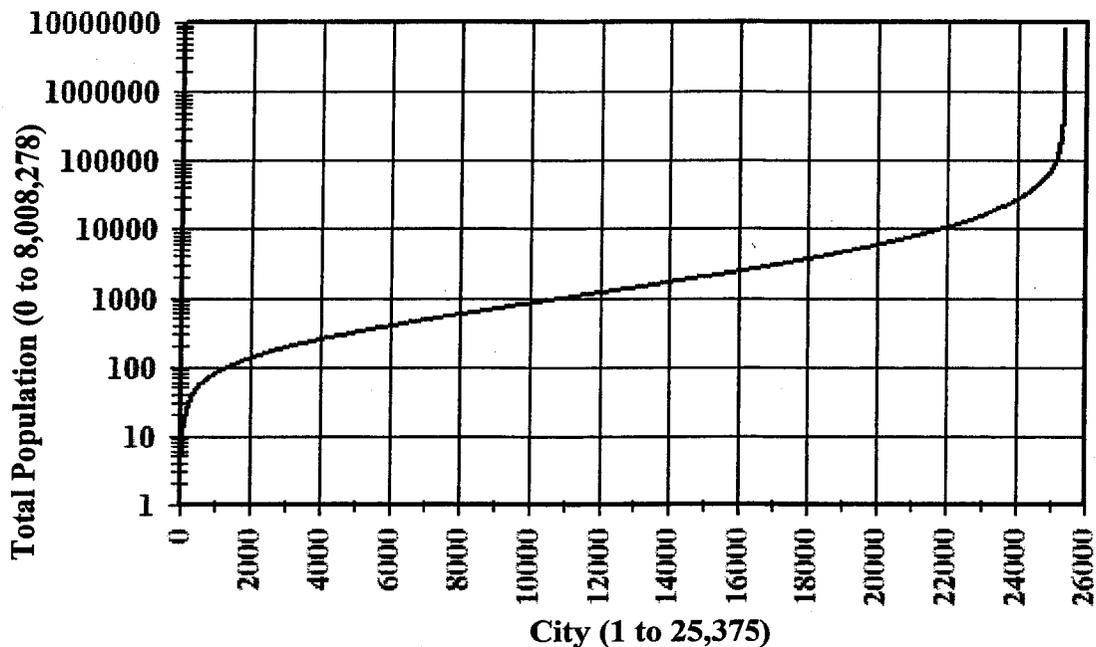


Figure 9 – Total Population, Baseline G2000 Place Name Data

The total population varies widely across the dataset from 0 (18 occurrences) to total populations over 1,000,000 (9 occurrences) as the plot above indicates. Since the vertical scale is Logarithmic and the curve still retains distinct “knees” at either end points out the non-linearity of the total population’s distribution in the G2000 dataset. Note that cutting off place names with 1,000 or less indicates nearly 11,000 (or about 1/3 of the total) records. At a cutoff of 10,000 almost 70% of the place names would be eliminated.

To study the effects of different population cutoff values (as well as the recommended City Circles) on the condensed set of Place Name data a custom software utility was devised. It is discussed, along with supporting graphs that show the sensitivity of varying the total population cutoff value, in the next section.



ECM and TCM Usage for HOS Solutions

3.2.3 Place Name Analysis Utility

To study the effects of different population cutoff and City Circle filtering effects for the Lower 48 states, a custom software utility was developed in Microsoft VisualBasic. The utility uses as input the baseline G2000 data and the recommended CC data as described in the previous sections. Figure 10 shown below is a screen shot of the utility with the recommended settings for the population and CC filters. Using 2500 for the population filter and turning on CC filtering reduces the place names from 25,375 to 6,482 (about 75%) which will significantly improve performance in the HOS solutions with lower memory capacity.

2000 Census Place Name Utility
✕

Place Name Incorporation

- City Place Name
- Town Place Name
- Village Place Name (Mostly VT)
- Census Defined Place (CDP) Place Name
- City and Borough Place Names (AK)
- Borough Place Name
- Municipality Place Name (Anchorage, AK)
- City Balance Place Names
- County Balance Place Names

File Statistics

- Cities: 3577
- Towns: 421
- Villages: 367
- Census Defined Place (CDP): 1716
- City and Borough: 0
- Borough: 392
- Municipalities: 0
- City Balances: 3
- County Balances: 6
- Total Place Names: 6482**

Gross Place Name Filters

Population Cutoff, do not include at < 2500

Filter Place Names Based on City Circle Data

48 Conterminous States Graticule Statistics

Num X Segs	1	12	25	35	50
Min	6482	114	26	18	12
Max	6482	1299	1007	932	587
Mean	6482.0	540.2	259.3	185.2	129.6
IndCnt	12	56	108	148	208
Min	22	0	0	0	0
Max	1272	500	418	572	337
Mean	648.2	54.0	25.9	18.5	13.0
IndCnt	48	488	1008	1408	2008
Min	5	0	0	0	0
Max	726	370	350	459	279
Mean	324.1	27.0	13.0	9.3	6.5
IndCnt	88	968	2008	2808	4008
Min	3	0	0	0	0
Max	553	323	240	374	227
Mean	216.1	18.0	8.6	6.2	4.3
IndCnt	128	1448	3008	4208	6008

Num Y Segs

1

10

20

30

Generate Simulation Files

Prepared for

by

Compute Statistics

Status Ready

Figure 10 – 2000 Census Place Name Utility set at Recommended Filter Values



ECM and TCM Usage for HOS Solutions

The setting at a population cutoff of 2,500 or less and to include the City Circles was determined by running the utility with the population cutoff value from 0 to 5,000 in increments of 250, with the CC filter both off and on. This resulted in the Table and graph, shown at the right in Figure 11.

When the cutoff is set to zero (no filtering) and the utility run with no City Circle filtering there are 24,654 records. This is less than the baseline of 25,375 and has been reduced by Alaska, Hawaii, Puerto Rico, and the eighteen 0 population occurrences which are not applicable to HOS solutions in HD vehicles running in the 48 Conterminous States.

As the cutoff value is increased the number of PN's drops down non-linearly at values of about 2,500 or less, reflecting the left side "knee" in the baseline curve in Figure 9. The City Circle effects can be gauged by the CC Delta column of in the table which is also the lower gray curve in the graph.

This indicates that, as expected, applying the City Circles eliminates over 3000 small communities. The difference between the CC effect (the 4th column in table in Figure 11) trends down as the small communities as their total population increases.

The upper two curves in Figure 11 follow the same shape indicating that the effects of the adding the City Circles is a linear one. The bottom curve confirms this as it is almost linear. Because the City Circle effects are linear we recommend that this filter be used for HOS solutions.

With this decision taken the remaining factor in setting the recommended Place Name dataset is what population cutoff to use. This is primarily a function of two factors. The first is to eliminate the smaller communities that are causing non-linear effects, and this indicates a cutoff of 2,500 at a minimum.

We can further condense the dataset by increasing the cutoff value, which effects the storage capacity of the HOS solutions. This will be the most acute in the Firmware solutions with lower persistent chip memory capacity. With 2,500 as the cutoff value, about 170KB of space is required for the resulting data, which is less than 3% of a firmware or PDA with an 8MB capacity.

Total Pop Cutoff	No CC Filter	With CC Filter	CC Delta	% Total w/CC Filter
0	24654	21340	3314	86.56%
250	20801	17574	3227	71.28%
500	17628	14515	3113	58.87%
750	15535	12527	3008	50.81%
1000	13959	11053	2906	44.83%
1250	12721	9881	2840	40.08%
1500	11715	8960	2755	36.34%
1750	10887	8200	2687	33.26%
2000	10145	7519	2626	30.50%
2250	9525	6967	2558	28.26%
2500	8965	6482	2483	26.29%
2750	8492	6077	2415	24.65%
3000	8073	5718	2355	23.19%
3250	7723	5423	2300	22.00%
3500	7385	5134	2251	20.82%
3750	7095	4894	2201	19.85%
4000	6825	4682	2143	18.99%
4250	6557	4472	2085	18.14%
4500	6339	4301	2038	17.45%
4750	6016	4127	1889	16.74%
5000	5912	3974	1938	16.12%

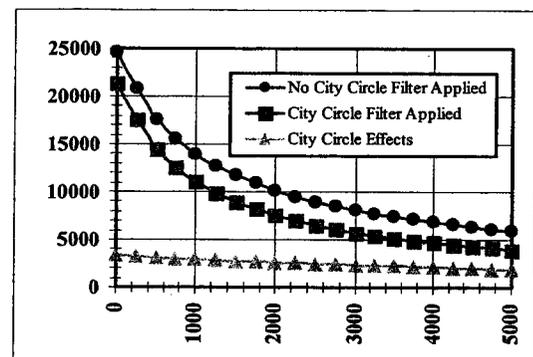


Figure 11 – PN Filter Parametrics

This study recommends that the 2,500 cutoff value be used for the Place Name Dataset.

This reduces the 25,375 records down to 6,482, 349, or 131 Place Names for the 48 States, Alaska, and Hawaii. The complete set of 6,482 Place Names were not printed for direct inclusion in this document but are available in two forms on the CD. The first is a structured Excel spreadsheet that contains the data as well as the formulae that applies the Lambert Conformal Conic projection to the angular measures. It is the “2000 Census Place Names.xls” file at:

D:\Place Name Data\2000 Census Place Names\2000 Census Place Names.xls

The data without the projection information and the projection rationale has been re-formatted for easier review and converted to PDF and is available in the Research Folder as “08 - Recommended 2000 Census Place Names for HOS Solutions.pdf”. The next section covers the determination of the recommended State Border Crossing dataset.

3.3 Recommended State Border Crossing Data Set for HOS Solutions

Developing the suite of SBC records was done differently from the Place Names. In this case the “filter” required is initially defined and requires no parametrics to quantify. The 1:2,000,000 DLG data is already posed with the road data trimmed to the state lines in the input. Because of this the endpoints of each polylines can be directly matched. The border entities are not required other than to check the results graphically.

First, only the unique edges adjoining two states need to be individually examined. For example in Virginia there are 7 different borders, 6 of which are applicable to HOS solutions. Figure 12 below shows the state and the attendant nomenclature.

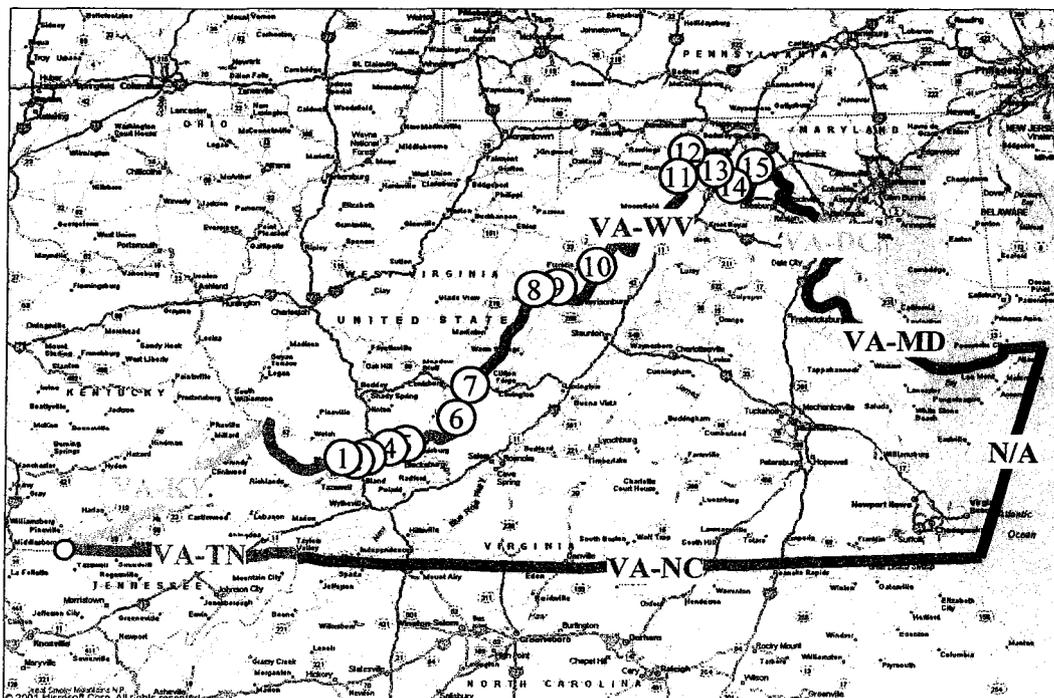


Figure 12 – State Border Crossing Nomenclature for Virginia



ECM and TCM Usage for HOS Solutions

The HOS edges are the 6 states that adjoin Virginia with the seventh the ocean border, marked as N/A in the figure on the last page. The crossings between Virginia and West Virginia for Interstate, Federal, and State roads are shown as the numbered circles in the figure. Map data may provide border crossings down to individual streets which would result in too many records for the HOS solutions.

Figure 13 at the right shows for the short stretch between number 1 and 2 on the figure on the last page. Examining this at the street shows four non-numbered roads that would probably not be added to the HOS dataset for SBC's level.

All the roads in each state are comprised of the polylines described previously. All states to not adjoin with each other and there are 226 unique state-to-state edges.

The 1:2,000,000 data discussed earlier is posed as polylines with label data first. To extract the SBC locations for the state-to-state locations only the Transportation file for each state was interrogated. The computation of all the SBC records for the HOS solutions was accomplished in 4 steps; the first two automated and the last two manually performed.

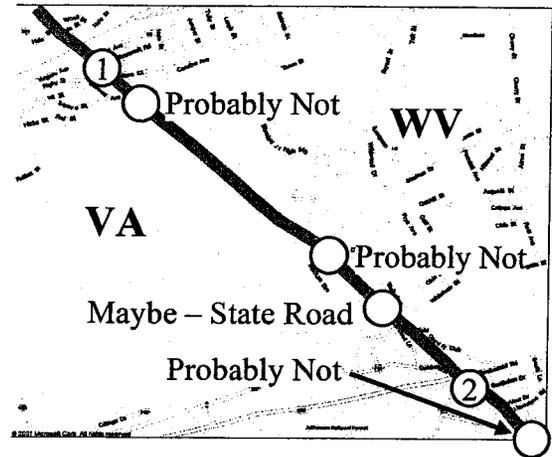


Figure 13 – VA/WV Example

3.3.1 Baseline Data Condenser Utility

The first step was to write a simple software utility to remove excess data from the baseline USGS 1:2,000,000 scale data. An example record in Virginia is:

```
DESCRIPTION=SECONDARY ROUTE, CLASS 2, SYMBOL UNDIVIDED
NAME=US17
ENTITY_LABEL=1700205
ROUTE_NUMBER=US17
ROUTE_NUMBER=US50
-78.090523,39.079346,0.0
-78.104624,39.085851,0.0
-78.114639,39.089136,0.0
-78.120368,39.099626,0.0
-78.124733,39.119620,0.0
-78.129254,39.131456,0.0
-78.136768,39.141964,0.0
-78.150259,39.150271,0.0
```

The characters marked in **Bold** are those needed for the downstream matching utility. The program reads in each state's data and extracts all the "ROUTE_NUMBER" data as well as the first and last Latitude/Longitude pairs. The converted record for the above is:

```
-78.090523,39.079346,-78.150259,39.150271,"US17/US50"
```



ECM and TCM Usage for HOS Solutions

New ASCII text files are created for each state with the condensed data. The slash “/” used between the route names indicates that both US 43 and SR 13 are both designated for this polyline. The state border point itself can only be at one end or the other of a polyline. Furthermore, the matching point in whichever adjoining state’s polyline will also be at one end or the other. Automated methods can search for these matches, uniquely identifying the SBC location.

This reduces the number of characters from 453 to 53 or 88% in the example above. Applied across all the data files for the 48 Conterminous States resulted in the next utility that extracts the matches.

3.3.2 State Border Crossing Matching Utility

The second step was another software utility that matches the condensed data for the 226 unique state-to-state borders. The utility has built-in logic to isolate the 226 edges to reduce processing time. The data is read into temporary arrays with each adjoining state’s polylines examined one at a time. When a point matches, the labels and Latitude/Longitude for each state is written to the extract file.

As each unique edge is processed a flag is set to avoid re-computing when the other state is processed. The aggregate data was written to a comma-delimited (.csv) file which was in turn read into Excel. The utility extracted 1,195 matches, some of which were redundant. The process marking and removing the data is described in the next section.

3.3.3 Removing Duplicate Matches

The 1,195 records were read into Excel and examined for duplicates. These duplicates almost always occurred when two or more polylines had a common point at the state border with the matching point in the other state being a single polyline end. This causes redundant matches for the state with the multiple polylines ends at the same position on the border.

The “Crossings wDups” Tab in the “Border Crossings.xls” spreadsheet in the “State Border Crossings” Folder on the attached CD shows the duplications marked in Red. They were determined by sorting the data and looking for redundant records manually. With the duplications identified the last step was to add in the in International SBC’s to Canada and Mexico – another manual process described in the next section.



3.3.4 Adding International SBC Records

The International borders were identified by plotting the 1:2,000,000 data and examining the appropriate edge manually. Two mapping programs were used for this, Global Mapper for the DLG data and Microsoft MapPoint for the visualizations and International labels.

An individual SBC to another country was identified in Global Mapper and the corresponding view in MapPoint visualized. The Global Mapper view provided the Labels for the route names in the United States while the MapPoint software provided the corresponding International route name(s) and the Latitude and Longitude at the crossing point.

The Alaskan/Canadian border has only 5 road crossings and the data for these was gathered manually. The Hawaiian Islands is an isolated land mass and it is assumed that HD vehicle tractors will move trailers on and sometimes between islands but not to the mainland. Because of this there were no state border crossing points considered for Hawaii.

The entire process was accomplished manually, the U.S./Canada border first, followed by the U.S. Mexican border, and finally the Alaskan/Canadian border. This increased the total number of records to 2,350 for the recommended SBCs.

3.3.5 Final Checks and Recommended SBC Dataset

As a final check this aggregate data was formatted ("Crossings 4Map" Tab in the Border Crossings.xls spreadsheet on the attached CD) and read back into Global Mapper. This superimposed all the crossing points with the Transportation and Boundary entities from the 1:2,000,000 data. This was visually inspected and indicated correct matches. The zoomed out view of this, plotted with the Lambert Conformal Conic projection and a zoomed in example on the FL/GA border is shown below in Figure 14.

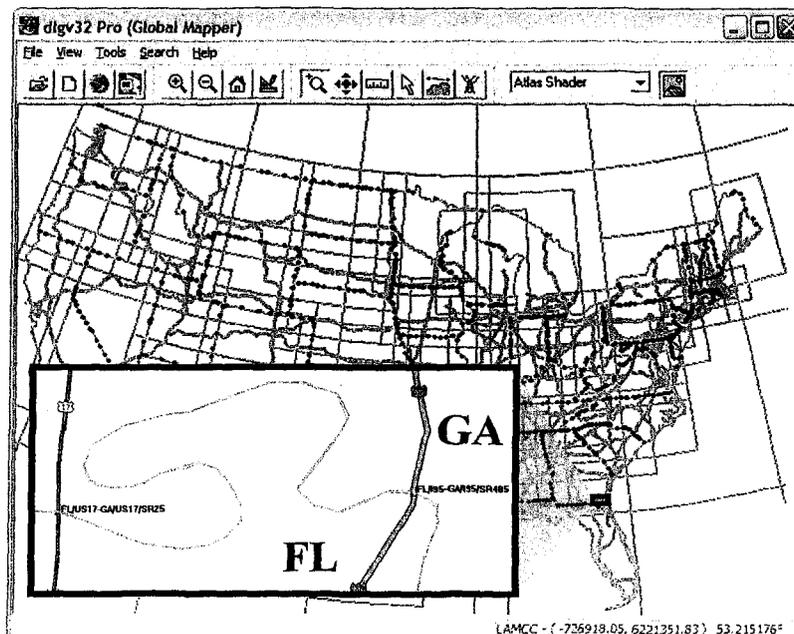


Figure 14 – State Border Crossing Results and Example



ECM and TCM Usage for HOS Solutions

The complete set of 2,345 SBC records were not printed for direct inclusion in this document but are available in two forms on the attached CD. The first is a structured Excel spreadsheet that contains the data as well as the formulae that applies the Lambert Conformal Conic projection to the angular measures. It is the "Border Crossings.xls" file at:

D:\ State Border Crossings\ Border Crossings.xls

The data without the projection information and the projection rationale only has been re-formatted for easier review and converted to PDF and is available on the attached CD in the Research Folder as "14 - Recommended State Border Crossings.pdf". The next section of this document covers the basic usage of this data for the main classes of HOS solutions.



SECTION 4 - PLACE NAMES AND STATE BORDER CROSSING DATA IN HOS SOLUTIONS

HOS solutions can be divided into three basic classes: Firmware, Portable CPU, and PC-Based. "Front-End" solutions are those that will reside in the vehicle during the trip and gather the data. "Back-End" solutions will be PC-based and both pre-load and recover the HOS data records before and after the trip.

4.1 Front End Solutions

"Front-End" Firmware solutions can use a CPU and the fixed datasets for Place Names and State Border Crossings on the vehicle. Some form of portable storage will hold the secure data that accumulates the HOS records. These solutions could, in general, possess the lowest power CPU's and also have the lowest storage capacity.

"Front-End" PDA solutions could carry the PN and SBC datasets and also store the HOS data records. These solutions would have significantly more computing power and storage capacity.

In either case the way the two recommended datasets are used depends on whether the vehicle has a GPS system connected to the CPU directly (or through the vehicle's Low or High Speed vehicle network) or there is no GPS data source for the solution.

"Front-End" Solution With GPS Data Source

These solutions will be able to provide a Latitude and Longitude whenever an HOS record is generated. The Lambert Conformal Conic projection could be applied which would yield X and Y coordinates that could use a simple table-lookup to recover the appropriate PN or SBC code.

"Front-End" Solution Without GPS Data Source

In this case there is no GPS system and the precise location of the vehicle would not be stored. Instead either a paper book, in simple solutions with only a basic keyboard, or software functions in solutions with touch screens or keyboards could be used to manually look up the location.

The numeric code would result which would be stored in the HOS record. In systems with only a numeric keypad the code would be looked up in a book and the code number entered by hand. Since the datasets contain the names, codes, and X,Y coordinates the computer can use inverse formulae to compute the Latitude and Longitude of the location of the PN or SBC if needed.

This will store the closest PN possible for the Driver Status Change or SBC event in the HOS record. The next section discusses PC-based back-end systems.



ECM and TCM Usage for HOS Solutions

4.2 PC-Based Back-End Portable CPU Solutions

PC-based solutions have much higher CPU and storage capacity and the PN and SBC datasets as recommended will easily integrate into these systems. The way the data will be used is different. In these systems the driver(s) will not be involved, rather the HOS records will be archived and/or reviewed.

The HOS record will hold a set of XY coordinates for each record. The PC could convert these values into Latitude and Longitude values which in turn could be used to plot the HOS records for a trip on a map to lend more context to the information graphically.

The higher performance and storage capacity could also allow the PC-based systems to refine the locations for HOS records recorded in systems with GPS. These records would have X,Y coordinates based on the more precise GPS input and could have any City Circle condensed Place Name augmented by a precise location from the latitude and longitude contained in the HOS data record.

This yields better context as any reviewer could see the exact location of the vehicle, probably displayed on a digital map. The use of more precise locations can be carried further with the 30-50 Meter accuracy of GPS-equipped solutions by allowing the Driver Status and State Border Crossing event locations to be plotted at street-level detail.

The next section presents our Recommendations for using the Place Name and State Border Crossing data in HOS solutions.



ECM and TCM Usage for HOS Solutions

SECTION 5 - RECOMMENDATIONS

Future HOS solutions will require both Place Name and State Border Crossing numeric codes to be included in records that electronically document a Driver Status Change or State Border Crossing. The following recommendations are related to these data sets.

The HOS solution software should compute the PN or SBC numeric code if there is an on-board GPS system in the vehicle. This will minimize tampering and provide the location for each Driver Status Change or State Border Crossing event.

Drivers should manually input the PN and SBC numeric codes if there is not an on-board GPS system. Although prone to tampering this is the only way to gather HOS information about where the Status Change and Border Crossings occur. The ECM and other tamper-resistant sources would provide the time and distance information to indicate HOS compliance.

A hierarchical input scheme should be used to recover the numeric code from software. The driver would input from high to low level of detail to identify the PN or SBC using state, city, and road names. Software would prompt for the state, then the city for PNs and the states on either side of the border crossing, then the road name for SBC events.

If the HOS solution only contains a numeric keypad, the same book used for the paper backup system should be used to manually look-up the numeric codes. This book would also be organized hierarchically with tabs by state; each section containing the PN and SBC codes.

The Census Bureau's "U.S. Gazetteer 2000" file should be used as a baseline for the HOS Place Name data. This baseline file with 25,375 Place Name records is documented on the attached CD in the research folder in the "06 - Complete 2000 Census Place Names.pdf" file.

The USGS "1:2,000,000 Digital Line Graph" data files organized by State should be used as a baseline for the HOS State Border Crossing data for borders between the Conterminous 48 states. These files contain state border and road information that can be processed via computer to yield over 90% of the SBC locations.

The World Geodetic System – 1984 (WGS 84) ellipse should be used for the Earth Datum for HOS Latitude/Longitude projections. The two WGS 84 parameters used are the semi-major axial distance (radius at the Equator) of 6378137 Meters and a Flattening factor of 1/298.257223563.



ECM and TCM Usage for HOS Solutions

The PN and SBC data should be projected using the Lambert Conformal Conic projection posed three ways, one for the Conterminous U.S., another for Alaska, and a third for Hawaii; as shown in Table 1. This will assure the best accuracy as the angular measures from the G2000 and 1:2M DLG datasets are converted to an XY grid. The grids are positioned in the lower left-hand corner of the three areas of interest, always producing positive position numbers for coordinates. This could allow the use of unsigned numeric encoding in the software which will produce better performance and use less data storage.

	Lower 48 States	Alaska	Hawaii
Projection	Lambert Conformal Conic	Lambert Conformal Conic	Lambert Conformal Conic
Datum	WGS 84	WGS 84	WGS 84
1st Std Parallel (DD)	33.000000N	51.833333N	20.000000N
2nd Std Parallel (DD)	45.000000N	53.833333N	21.125000N
Latitudinal Origin (DD)	24.559166N	51.883419	19.065925N
Longitudinal Origin (DD)	124.615672W	176.645061W	159.716290W

Table 1 – Recommended Latitude/Longitude to Grip Projection Parameters

Place Name data from the G2000 dataset should use a total population cutoff filter set at 2,500 for the Conterminous U.S. This significantly reduces the data storage required in the HOS solution while still retaining significantly sized place names for HOS record incorporation.

“City Circles” should be used to further reduce small communities in large cities from the recommended PN dataset for the Conterminous U.S. This will provide data with better context for HOS reviewers. The 129 recommended cities and their data are documented on the attached CD in the Research folder in the “07 - Recommended City Circles for HOS Solutions.pdf” file.

No “City Circle filtering should be used for data concerning Alaska and Hawaii. These states have 395 and 131 place names respectively in the G200 baseline data and would easily fit in HOS solutions tailored for HD vehicle operations in these two states.

With the above Population Cutoff and City Circle filters applied the Recommended HOS solution Place Name dataset should be used in “front-end” HOS solutions. The 6,962 recommended place names and their associated data are documented on the attached CD in the Research folder in the “08 - Recommended 2000 Census Place Names for HOS Solutions.pdf” file.

The State Border Crossing data based on USGS 1:2M DLG with International border crossings added should be used for “Front-end” HOS solutions. The 2,350 recommended state border crossings and their associated data are documented on the attached CD in the Research folder in the “14 - Recommended State Border Crossings.pdf” file.

“Back-end” HOS solutions should use unfiltered Place Name data augmented by street-level map plotting. This will allow reviewers to plot records from HOS solutions on vehicles with GPS for the best possible context.



ECM and TCM Usage for HOS Solutions

BIBLIOGRAPHY

The 14 documents used in the research are listed below and on the next page. Portable Document Format (PDF) is used. All the listing except the first two, which are text books, are included on the CD-ROM for this module.

#	Title
1	USGS – Map Projections Used by the U.S. Geological Survey, Geological Survey Bulletin 1532
2	CRC - Standard Mathematical Tables, 27 th Edition
3	USGS - GNIS Metadata Structure
4	FIPS - 55-DC3 - Codes For Named Populated Places, Primary County Divisions, and Other Locational Entities Of The United States, Puerto Rico, and the Outlying Areas
5	BoC – 2000 U.S. Gazetteer Guide
6	Generated – Complete 2000 Census Place Name Data
7	Generated – Recommended City Circles for HOS Solutions
8	Generated - Recommended 2000 Census Place Names for HOS Solutions
9	EuroControl - WGS 84 Implementation Manual, Version 2.4
10	USGS - Standards for 1:24,000-Scale Digital Line Graphs-3 Core
11	USGS - USGS Digital Line Graph Data Overview
12	USGS - Standards for the Preparation of Digital Geospatial Metadata
13	USGS - Standards for Digital Line Graphs
14	Generated - Recommended State Border Crossings Data



Federal Motor Carrier Safety Administration

Office of Business and Truck Standards and Operations

Research and Analysis on the Paper Backup System for HOS Solutions

January 21, 2003



Paper Backup Systems for HOS Solutions

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
TABLE OF CONTENTS.....	II
SECTION 1 – EXECUTIVE SUMMARY.....	3
SECTION 2 – FORMS, INSTRUCTIONS, AND PLACE NAME DIRECTORY IN THE VEHICLE	4
2.1 Forms Kit and Instructions.....	4
2.2 Notional Book Format for PN and SBC Codes.....	4
SECTION 3 – DATA CONSOLODATION ISSUES.....	6
3.1 Use of Optical Character Recognition (OCR) in Back-End Solutions	6
SECTION 4 - RECOMMENDATIONS.....	9
BIBLIOGRAPHY.....	10



Paper Backup Systems for HOS Solutions

SECTION 1 – EXECUTIVE SUMMARY

Section 395.15 of the FMCSA Regulations requires a paper backup system in the event that the automated HOS solution fails. In the event of Electronic On-Board Recorder (EOBR) failure, drivers must revert to the requirements of Section 395.8 of the FMCSA Regulations and reconstruct their lost record of duty status and manually record the remainder of the current trip duty status.

Supporting both the failure of an EOBR HOS Solution and the notional data record described in previous modules, could be a directory containing Place Name (PN) or State Border Crossing (SBC) numeric codes. The Place Name data could be organized in a directory, alphabetically by state and then city, implementing the same notion as in phone books. With approximately 7,000 Place Names and 50 states, each state could be fully listed in one or two pages. The State Border Crossing records could use tables that isolate unique state-to-state border segments to minimize the time for looking up the crossing code. This would yield 1-3 pages for each state, again using a hierarchal listing.

The paper backup system records could be transcribed into back-end HOS solutions at the end of a trip. This could be accomplished using manual or automatic techniques. Small motor carrier operations may not need to automate the transcription, while larger operations that have more information to transcribe may want to automate.

The use of Optical Character Recognition (OCR) technology could be used to accomplish this automation if desired. Scanner hardware ranges from a single sheet flatbed scanner to 80 pages per minute machines featuring unattended operation. A user would invoke the appropriate software function in the back-end HOS solution, load the forms, press or click to start, and allow the Optical Character Reader (OCR) device to scan the data. After reviewing the information the HOS records would be stored.

In general, the use of OCR to automate the transcription of paper backup data sets will need a cost-benefit analysis. Organizations should first gage the failure rate of the automated HOS front-end solutions and the labor required to manually transcribe the volume of information before making the investment in hardware, software, training, etc.



Paper Backup Systems for HOS Solutions

SECTION 2 – FORMS, INSTRUCTIONS, AND PLACE NAME DIRECTORY IN THE VEHICLE

FMCSA Regulation Section 395 requires a backup system in the event that the automated HOS solution is not available. This paper system could be supplied in the vehicle as a kit containing instructions, forms described in Section 395.8 of the FMCSA Regulations for recording drivers duty status, and a directory code book to manually lookup the codes for PN or SBC locations.

Vehicles without GPS systems and a HOS solution with the minimum numeric keypad for input will require a code book to manually lookup the codes for PN or SBC locations. The code book will enable a driver(s) to enter the proper code into the HOS solution via a keyboard. The book could also be directly used in the paper backup system in the event of an EOBR system failure.

2.1 Forms Kit and Instructions

As required by FMCSA Regulations, Sections 395.15 (f) and (g), “drivers are required to note any failure of automatic on board recording devices, and to reconstruct the driver's record of duty status for the current day, and the past 7 days, less any days for which the drivers have records, and to continue to prepare a handwritten record of all subsequent duty status until the device is again operational. The forms kit must have available sufficient copies of the driver duty status forms for each 24 hour period of duty during their assigned trip.”

Subparagraph (g) goes on to require each commercial motor vehicle to must have on-board the commercial motor vehicle an information packet containing the following items:

An instruction sheet describing in detail how data may be stored and retrieved from an automatic on board recording system; and

A supply of blank driver's records of duty status graph grids sufficient to record the driver's duty status and other related information for the duration of the current trip.

2.2 Notional Book Format for PN and SBC Codes

The “Research and Analysis on Using Geo-Referenced Data in Hours of Service Solutions” module previously delivered developed notional data files for the Place Name and State Border Crossing items. These files contain a superset of the information that could be provided in a code book that would be included with the paper backup system. The “Research” folder on the attached CD contains these files in the “01 - Notional 2000 Census Place Names for HOS Solutions.pdf” and “02 – Notional State Border Crossings.pdf” files respectively.

The Place Name data could be organized alphabetically by state and then city. This implements the same notion as is used in phone books and dictionaries. With the approximately 7,000 Place Names and 50 states, each state should be fully listed in one or two pages.

A notional Place Name page was developed for the state of Virginia. Virginia has 131 Place Names and with a 10 point non-proportional font and three columns fits on a single page. The



Paper Backup Systems for HOS Solutions

layout implies that there would be approximately 150 Place Names per page and for approximately 7,000 place names for the USA it would take 47 pages for the entire book with 1 or 2 pages per state. A notional depiction of the Place Name arrangement was developed and is available in the "Research" folder on the attached CD on the first page of the "03 – Place Name Book Example - VA.pdf" file.

Effectively organizing the State Border Crossing records could use tables that isolate unique state-to-state border segments to minimize the time for looking up the crossing code. The book could be organized with 1-3 pages for each state, again using a hierarchal listing. Sets of tables could be used to isolate the borders between the states of interest with the information sorted by the route name and the nearest location to facilitate looking up the numeric code.

A notional State Border Crossing page was developed for the state of Virginia and is listed for review in the "Research" folder on the CD on the second page of the "06 - State Border Crossing Book Example - VA.pdf" file.

The data could also be related using a map plot of the isolated border in place of the table that is sorted by the nearest location. Figure 1 at the right shows a notional example for the Virginia-Kentucky border segment.

The 5 crossings are shown both in the table and on the map with the direction of travel out of the state shown with an arrow. The route name (Kentucky in this example) is shown with a slash and then the code.

Individual border crossings would be shown in their true positions, allowing the numeric code to be identified and added manually to the event record. This allows the driver to either use the table or the map for finding the code.

In areas where there are concentrations of crossings a magnified inset of the map could be used to show the required detail. In most cases the route names in both states are the same, allowing a simpler labeling scheme. In Figure 1 above, all but 1 of the 5 crossings have the same name which allows a simpler table layout to be used. The notion is to allow the driver to lookup the State Border Crossing numeric code by reading a map or a table and directly entering the information.

After a trip is completed the records will need to be recovered to a back-end system and stored; the next section covers that process.

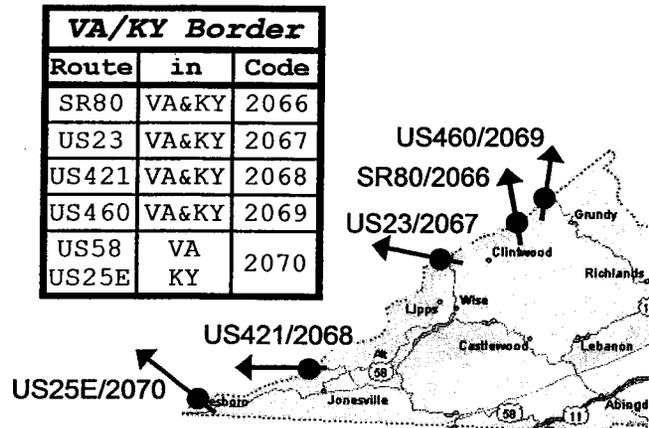


Figure 1 – SBC Example for VA-KY Border



SECTION 3 – DATA CONSOLIDATION ISSUES

HOS solutions should use an open standard to allow different front-end and back-end solutions to be interchangeable. This was recommended for the notional data record and carries through to the paper backup system's use of a common form with data items that emulate the HOS digital record. This will allow a back-end system, whether used by the carrier or a roadside inspector, to indicate compliance for any automated or paper backup system.

Any data gathered by the paper backup system as a result of an HOS solution failure will be transcribed into the back-end HOS solution, completing the data recovered for a trip. The way this is accomplished could span the range from completely manual to completely automated. Regardless of the technique used, the notional forms presented in the last section could be used.

Small operations may not need the ability to automate his transcription process. The back-end solution used in these small operations would need a function that allows data to be entered manually, allowing the information recorded on the forms to be incorporated.

Larger operations that have to transcribe more information may want to automate the process. The use of Optical Character Recognition (OCR) technology could easily accomplish this. The next section describes the three commonly used classes of this technology.

3.1 Use of Optical Character Recognition (OCR) in Back-End Solutions

The OCR technology applicable to HOS solutions would employ a single class of software that could be run on a personal computer (PC), using a peripheral scanner to read the handwritten data from the forms, converting to data. The notional forms presented earlier include 2 pages for initial information plus at least 2 more for reconstructed and post-failure HOS data, for a minimum total of 4 pages that would have to be transcribed.

Basic research with numerous Commercial Off-The-Shelf (COTS) found that vendors provide OCR software that could be used for HOS solutions. Three examples are Caere Software, Cardiff Software, and Kofax Image Products that provide a full range of OCR COTS that could be used for HOS solutions. On the attached CD references 7 through 16 in the "Research" folder relate product description and some tutorial "white papers" about semi- and fully-automated OCR solutions

All three classes could use the COTS software from the manufacturers mentioned earlier as their products include Application Programming Interfaces (APIs) that would allow the HOS back-end software to command a scanner to recover the data from the forms.



Paper Backup Systems for HOS Solutions

The three classes from a hardware perspective are generically shown in Figure 2 below.

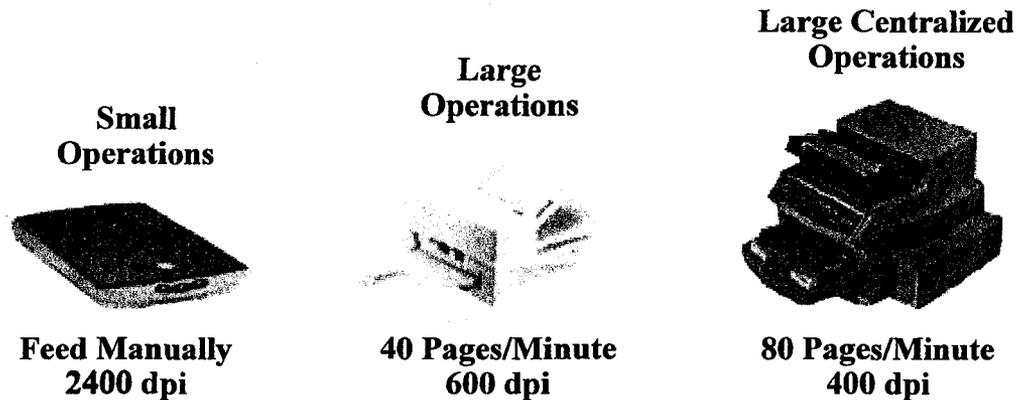


Figure 2 – Three Classes of OCR Hardware

The 1st class of hardware is the Flatbed scanner. These devices are the least expensive of the three classes and require the user to manually place document, one page at a time, in the scanner and then take some action on the PC. OCRs typically scan at 150-300 dots per inch (dpi, also called the resolution) which provides enough detail for the recognition processing while maximizing the speed that the page is scanned.

The Flatbed scanners typically offer much higher resolutions with 2,400 (about 8 times more than is needed) the standard. The devices typically are connected directly to a PC. The user would invoke the back-end HOS solution function and manually feed each sheet when prompted, reviewing the scanned information for OCR error correction. Small operations that only occasionally need to transpose a backup paper set of HOS records could use this class of hardware.

The 2nd class of hardware further automates the process with a sheet feeder that would typically accept a single set of HOS paper backup forms. This class of device will scan about 40 pages per minute (ppm) which implies an 8 page backup record would scan in about 12 seconds.

The user would invoke the appropriate software function in the back-end HOS solution, load the forms in order, press or click to start, and allow the OCR device to scan the data. After scanning the information would need to be reviewed for recognition errors and then stored. This class of hardware is more expensive that the 1st class and would only be applicable in large operations that generate enough paper datasets to warrant its use.



Paper Backup Systems for HOS Solutions

The 40 ppm scanning rate can be doubled in the third class of hardware the scans about 80 ppm. These devices are the most expensive of the three classes and usually dedicated for forms scanning and have high capacity feeders. The form factor of the machine is comparable to a Xerox machine and would only be applicable in very large operations that would centralize the processing of paper backup records. On the attached CD references 17-19 in the "Research" folder have some examples of these hardware items.

In general the use of OCR technology to augment the transcription of paper backup data sets will need a careful cost-benefit analysis. Organizations should first gage the failure rate of the automated HOS front-end solutions and the attendant labor required to manually transcribe the volume of information. In addition to the OCR hardware other costs are involved in periodic software licensing for the higher-end solutions.



Paper Backup Systems for HOS Solutions

SECTION 4 - RECOMMENDATIONS

The following recommendations are presented with respect to the use of the Paper Backup System as required by FMCSA Regulation Section 395.

At the point of failure have the driver(s) reconstruct the lost HOS records following the guidelines of FMCSA Regulation Section 395.8. This will recover this information with the maximum quality as the minimum time will have passed.

Utilize a simple to use book to facilitate the drivers looking up the numeric codes for Place Names and State Border Crossings. The book should include the same codes as would be used by the automated system.

Organize the book by state with alphabetical listings for the PN or SBC code as in a phone book. This will allow quick use by the data enterer.

Consider automated transcription of the manually recorded HOS records if the cost-benefit warrants. Organizations should first gage the failure rate of the automated HOS front-end solutions and the attendant labor required to manually transcribe the volume of information.

Conduct further research into the availability and applicability of specialized commercial off-the-shelf scanning software. This software could enable a motor carrier to scan FMCSA Regulation Section 395.8 driver's logs into their application software.



BIBLIOGRAPHY

The 17 documents used in the research are listed below and on the next page. A Portable Document Format (PDF) is used. The entire listing is included on the attached CD-ROM for this module.

#	Title
1	Notional 2000 Census Place Names for HOS Solutions
2	Notional State Border Crossings for HOS Solutions
3	Notional Place Name Book Example for VA
4	Notional State Border Crossing Book Example for VA
5	Caere Software - OmniForm Developer Description
6	Caere Software - OmniForm Product Sheet
7	Cardiff Software - Open Standards for eForm Management
8	Cardiff Software - Implementing eForms and Digital Signatures
9	Cardiff Software - LiquidOffice Product Sheet
10	Cardiff Software - TELEform Product Sheet
11	Kofax Image Products - Ascent Capture Product Sheet
12	Kofax Image Products - Distributed Data and Document Capture
13	Kofax Image Products - Merging Document and Data Capture
14	DocuLabs - Kovad Virtual Rescan Assessment
15	Canon - CanoScan D1250 - FB Scanner Product Description
16	Fujitsu - FI-4340C - 40 ppm Scanner Product Description
17	Bell and Howell - 8125D - 80 ppm Scanner Product Description



**Federal Motor Carrier Safety
Administration**

Office of Business and Truck Standards and Operations

**Research and Analysis on High-Level
Architectures for EOBR HOS
Solutions**

January 21, 2003



High-Level Architectures for HOS Solutions

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
TABLE OF CONTENTS.....	II
SECTION 1 – EXECUTIVE SUMMARY.....	3
SECTION 2 – HOS COMMON ARCHITECTURE.....	4
SECTION 3 – HOS SOLUTION HARDWARE.....	6
3.1 Paper Backup Front-end System	6
3.2 Front-end Solutions	6
3.2.1 Firmware Solutions with GPS.....	7
3.2.2 Firmware Solutions without GPS.....	8
3.2.3 PDA Solutions with GPS	8
3.2.4 PDA Solutions without GPS	9
3.2.5 Current COTS Products.....	9
3.3 Back-end Solutions by Mode of Operation.....	9
3.3.1 Large Operator Back-end Solution.....	9
3.3.2 Small Operation Back-end Solution.....	9
3.3.3 Owner-Operator Solution.....	10
SECTION 4 - RECOMMENDATIONS.....	11
BIBLIOGRAPHY.....	12



High-Level Architectures for HOS Solutions

SECTION 1 – EXECUTIVE SUMMARY

Previously, this effort has delivered four Research and Analysis Modules regarding automated Electronic On Board Recorder (EOBR) HOS solutions. They have all contributed to an integrated concept for the notional HOS Architecture presented in this document.

The key to a flexible and cost effective architecture is a common standard for HOS data records format, protocol, and security which was discussed in the Module 1 report “Research and Analysis on Hours of Service (HOS) Data Record Structure and Data Security.”

The second Module “Research and Analysis on Engine Control Module and Transmission Control Module Usage for Hours of Service Solutions” explored ways to minimize tampering and maximize automation, the in-vehicle engine control module (ECM). The analysis also suggested that (if available) a Global Positioning System (GPS) should be utilized for automated data gathering in forming the HOS data records.

A notional set of Place Name (PN) and State Border Crossing (SBC) codes was articulated in the third module “Research and Analysis on Using Geo-Referenced Data in Hours of Service Solutions.” A common standard was recommended for the PN and SBC requirements of FMCSA Regulation, Section 395.15 should be used and implemented using numeric codes. This could assure a common suite of PN and SBC locations.

The fourth module, “Research and Analysis on the Paper Backup System for HOS Solutions” proposed a common format for books that relate the numeric codes. The existing paper system (described in FMCSA Regulation, Section 395.8) for logging driver record of duty status could be used to augment an EOBR HOS solution in the case of a system failure.

The research and analysis accomplished in the modules described above was used to develop the common EOBR HOS architecture described in this document. It has a common logical and physical construct, allowing the in-vehicle (or Front-end) portions of the system from any vendor to communicate HOS data records to any carrier-based (or Back-end) system that would pre-load and recover the trip information. Specific implementations of the various classes could use a wide variety of hardware and software development tools.

Front-end solutions could range from simple firmware devices with records stored in ultra-portable media (SmartCards, flash memory, etc.) to simple portable CPU solutions (Palm, Pocket PC, WinCE) to commercial off-the-shelf (COTS) products. Three modes of operation for these Back-end systems are envisioned:

- 1. Large Operations** could use a single repository, interfaced by a network or on the Web, to a series of terminals at the local offices that communicate with the Front-end devices.
- 2. Small Operations** could use a scaled down version of this for with one or a few vehicles and a single Back-end machine could provide a cost-effective solution for that situation.
- 3. An Owner-Operator Solution** for single vehicles could use small laptop or PDA to combine the front- and Back-end notions into a single device for HOS data gathering and storage.

Officials performing inspections in the field could continue to use existing enforcement procedures. They would physically observe the HOS solutions built-in HOS Compliance check to gage any required enforcement actions.

SECTION 2 – HOS COMMON ARCHITECTURE

The overall EOBR HOS Architecture should utilize a common data record format to make future vendors of the Front-end (in the vehicle) and Back-end (at the carrier operation) as interchangeable as possible. This would result in the most efficient (from an IT perspective) HOS architecture as possible.

Figure 1, shown below, depicts an overall notional architecture for an EOBR HOS solutions.

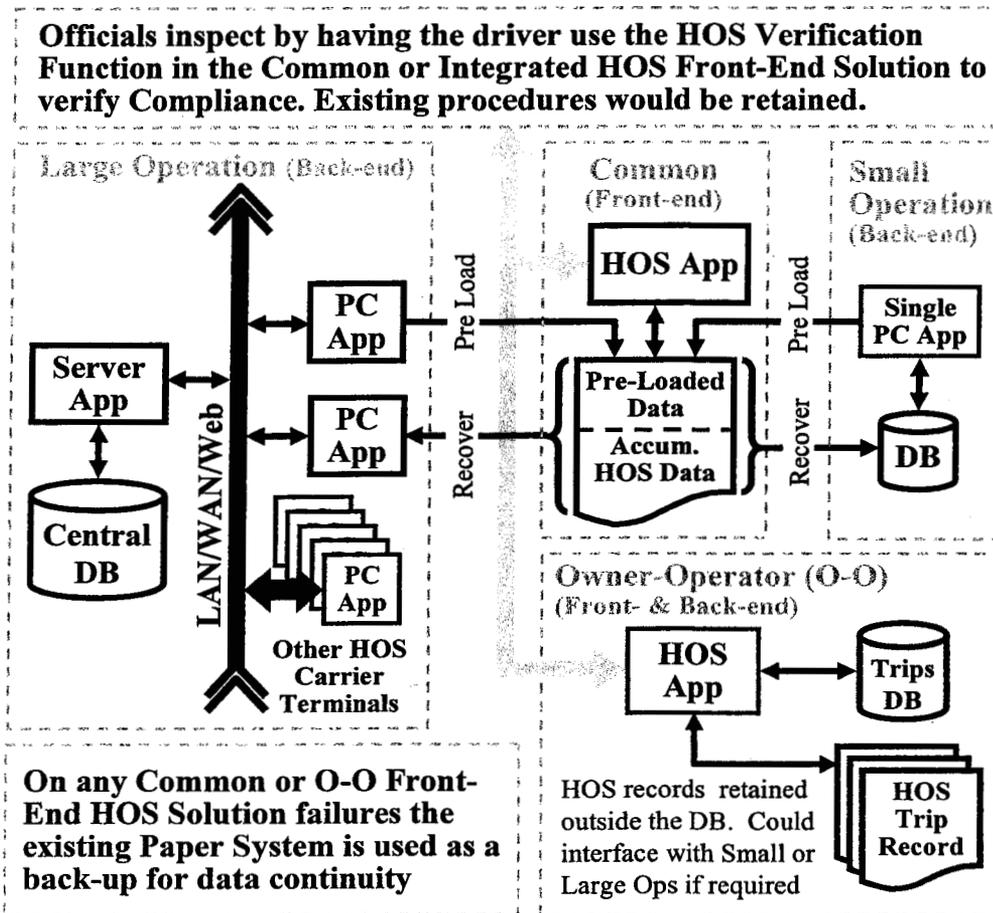


Figure 1 – Notional HOS Architecture

The HOS data record is contained in the document flow chart symbols in the center and at the lower right-hand portion of the figure. This could be the notional 24 byte record developed in the second module analysis that covered data record content and security. This applies to the Front-end solutions that are used in the vehicles to record the HOS data. These are labeled “Common” (as they can interface with any of the other three types if required) and “Owner-Operator” in the middle and lower right-hand portion of the figure.



High-Level Architectures for HOS Solutions

Three modes of operations are envisioned:

The first could be **Large Operations** with many Front-end solutions in the vehicles and a single centralized database at the carrier that stores the accumulated HOS records. Personal Computer (PC) terminals could be used at the local carrier's operations to pre-load the Front-end system that would then make the trip, accumulating the HOS data. At the end of the trip the same (or any other) PC terminal would recover the accumulated HOS data and move it to the centralized database. A local area network (LAN), wide area network (WAN), or the internet could be used to connect the centralized database and its server with the PC terminals at the local offices. The large operation is depicted in Figure 1 at the middle left.

The second could be **Small Operations** with a single PC-class computer that would both pre-load and recover the data from one or a few vehicles with common Front-end systems. This assumes that the operation has only a few vehicles that start and end their trips at the same locations. The software used could retain many of the same database and utilities as the Large Operation solution has, but a scaled down version might be used for the smaller trip rates and data storage requirements. No LAN or internet infrastructure is required as the Back-end system is a single computer. The small operation is depicted in Figure 1 at the middle right.

The third mode of operation concerns single vehicle **Owner-Operators**. In this case the entire HOS solution, front- and Back-end, could be integrated into a single device. The data capacity of the device would have to meet the six-month data retention requirement of FMCSA Regulation, Section 395 which could be accomplished in a small laptop computer, PDA or other device whose storage capacities approach 1GB. The HOS data record format should be retained in these systems to allow them to be used as a Front-end only system if the owner-operator performs services for a small or large operation with a Back-end component. The Owner-Operator solution is depicted in Figure 1 at the lower right.

Regardless of the mode being used the Common Front-end solution could interface with the Back-end portion of any of the three modes described above. This would allow small operations using a Common or Owner-Operator solution in the vehicle to seamlessly interface with a Small or Large Operation for vehicle trips. Likewise, any vehicle with a Common Front-end solution could communicate with any Back-end Owner-Operator solution used by single vehicle owner-operator that might periodically outsource a single trip.

All of the in-vehicle systems should be required to have a built-in function to inform the driver about his compliance status. Field inspectors would physically observe this function being run on the vehicle's system and document as necessary. The existing documentation system used by the inspectors would be retained.

If any of the in-vehicle HOS systems were to fail the existing paper system could be used to record the HOS data, the notion being that the record of the drivers duty status would be transcribed after the trip and then be stored in the Back-end or Owner-Operator systems data system.

The next section describes options for the hardware that could be used in the architecture of Figure 1.



SECTION 3 – HOS SOLUTION HARDWARE

The last section described three modes of operation that could encompass HOS solutions. Any Front-end component could interface with any Back-end component, resulting in maximum flexibility.

The next section covers the Paper Backup System, used if a failure occurs during a trip.

3.1 Paper Backup Front-end System

If any of the in-vehicle hardware components fail, the existing paper backup system (described in FMCSA Regulation, Section 395.8) could be used to reconstruct the missing data for downstream storage of the HOS compliance information. For the large and small operation modes, the pre-loaded information would be available from the Back-end system that initially stored that information before the trip started. The data reconstructed would cover the driver status change and state border crossing events. Owner-Operator Solutions would handle this data recovery on a trip by trip basis.

Paper backup records would be transcribed into Back-end HOS solutions at the end of a trip. This could be accomplished using manual or automatic techniques. Small motor carrier operations may not need to automate the transcription, while larger operations that have more information to transcribe may want to automate.

The use of Optical Character Recognition (OCR) technology could accomplish this automation if required. Scanner hardware ranges from a single sheet flatbed scanner to 80 page per minute machines featuring unattended operation. A user would invoke the appropriate software function in the Back-end HOS solution, load the forms, press or click to start, and allow the OCR device to scan the data. After reviewing the information the HOS records would be stored.

In general, the use of OCR to automate the transcription of paper backup data sets will need a cost-benefit analysis. Organizations should first gage the failure rate of the automated HOS Front-end solutions and the labor required to manually transcribe the volume of information before making the investment in hardware, software, training, etc.

3.2 Front-end Solutions

The in-vehicle portion of the HOS solutions could utilize a wide-range of hardware and software. Within the three modes of operation hardware ranging from firmware (simple device with portable memory) to fully contained Personal Data Assistants (PDA's) to Personal Computers (PCs) could be used. This implies a mapping between the modes of operation and the hardware classes that could implement them. Table 1, shown in the next page, depicts this mapping.



High-Level Architectures for HOS Solutions

Mode	Hardware See Section	Front-end Component					Current COTS	Remarks
		Firmware		PDA		WinCE		
		3.2.1	3.2.2	3.2.3	3.2.4	3.2.5		
		With GPS	No GPS	With GPS	No GPS			
Large Ops	Many	X	X	X	X	X	"Common" Solution in Figure 1 can interface with any Front-end component	
Small Ops	Few or 1	X	X	X	X			
Owner-Operator	1			X	X		"Owner-Operator" solution in Figure 1 Combined in 1 device	

Table 1 – Mode to Hardware Class Mapping

There are only four blank cells in the table, indicating that most modern devices could be used for all three modes of operation. The firmware solution that uses a simple dedicated in-vehicle keyboard would not easily allow the Back-end portion to be implemented, making an Owner-Operator solution infeasible. Likewise, the high cost of COTS systems used to optimize large operations would probably not apply to Small Operations and Owner-Operators situations.

The next five sections step through the Front-end hardware classes.

3.2.1 Firmware Solutions with GPS

The firmware hardware class encompasses the least complex of the HOS solution. The physical device could be permanently mounted in the vehicle with wired interfaces to the ECM and GPS units to provide automated HOS data record contents. The keyboard would only need basic function keys to input the driver status change codes as the GPS provides the latitude and longitude.

The driver is issued a SmartCard or some other portable storage item at the beginning of trip with preloaded data in place. At each status change the driver would input the appropriate status and the firmware device would gather the GPS and ECM data as needed, forming the HOS record which is then securely stored. After the trip the storage device is turned in and interfaced to a Back-end component with a reader that archives the records. In Large Operations the data would be moved forward directly to the repository.

The PC could erase and write to the card thereby, allowing re-use of the storage device again and again. Alternatively, the data device, if cost effective, could be retained as a physical data backup. Certain types of storage media like SmartCards could also be personalized (driver picture, barcode, etc.) to serve as an ID card as well.

3.2.2 Firmware Solutions without GPS

The firmware solution without GPS is very similar to the GPS enabled solution except that the locations would be provided manually with the driver looking up the appropriate numeric code as needed and entering it with a 0-9 numeric keypad. Figure 2 below shows a notional firmware device with the basic functions noted.

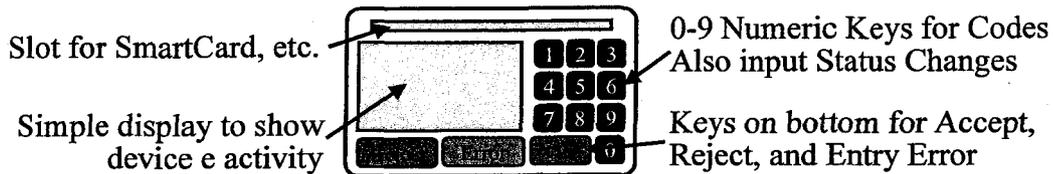


Figure 2 – Notional Firmware Layout (No GPS)

3.2.3 PDA Solutions with GPS

A PalmOS or PocketPC PDA device could be used to provide the Front-end system with two components – the PDA itself and a docking station installed in the truck. The docking stations have wired interfaces to the ECM and GPS and also provide power to keep the PDA batteries charged. All buttons for status change are “tapped” on the PDA screen using a standardized Graphical User Interface (GUI). Configurations from simple docking stations to adjustable view angles with printers are widely available as shown in Figure 3 below.

The driver interface could be very similar to the Firmware notion, but with more flexibility. The PDA’s touch sensitive screen would allow the buttons to be formatted and displayed with software, allowing a single software application to detect the presence of GPS and change the GUI accordingly for numeric code determination.

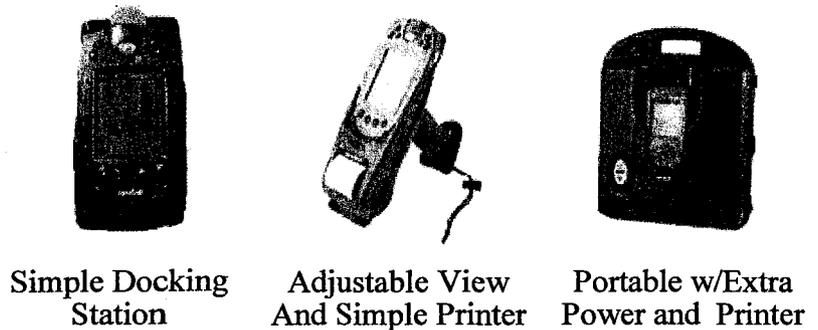


Figure 3 – Representative PDA Form Factors

A PDA could be docked when issued, when in-vehicle, and when the data is recovered, a “hot link” script would route the data to a local proxy space in the recovering PC, be processed to fill in the HOS details, and the results passed on to the Back-end repository. The “beaming” function in PDAs could also be used at the beginning and the end of the trip to eliminate brand-specific pin-outs from causing interface problems.

The driver(s) are issued a PDA, preloaded with the appropriate data at the start of the trip. At each status change the driver would input the appropriate status and the firmware device would gather the GPS and ECM data as needed, forming the HOS record which is then securely stored. After the trip the storage device is turned in and interfaced to a Back-end component with a reader that archives the records. In Large Operations the data would be moved directly to the repository.



3.2.4 PDA Solutions without GPS

If there is no GPS in the vehicle, a fixed PN and SBC database in the PDA could allow the driver to rapidly pick from drop-down menus first for the state, then road type (interstate, federal road, etc.), road number to indicate the location. The nearest Place Name could also be recovered from the database providing all the required information in the HOS records for the trip.

3.2.5 Current COTS Products

These solutions are complex COTS products that are currently available from numerous vendors. Most of these systems do not appear to support trip logs and HOS compliance data gathering, but are concerned with delivery and schedule logistics.

Many of these solutions utilize both GPS and some data exchange capability with a central carrier facility to allow communications (load, routing, vehicle status, etc.) with the vehicle. Frequently these devices are older Windows CE and HOS would probably entail the vendor assigning a HOS function to the solution. These solutions will probably not be useful for Small Operations and Owner-Operators as the high cost does not provide enough operational benefit.

3.3 Back-end Solutions by Mode of Operation

The three modes of operation described earlier are covered in the next three sections

3.3.1 Large Operator Back-end Solution

Large fleet operations would probably use a centralized repository for HOS data. The data could be recovered at the carriers local offices in standard HOS data records, and moved forward without user intervention. Some sort of LAN or Internet infrastructure would be required to interface the Back-end terminals. A single GUI-driven application in one or more PCs at the local offices that both pre-loads and recovers the data in any type of Front-end solution is recommended. The application could also be able to search the repository and recover historical records.

For a large operation that will analyze the HOS data to optimize their overall fleet performance, the ability to recover records from the central repository in a generalized sense via a LAN or the internet could also be used. If the internet is used, either an InterNet or IntraNet paradigm could be used to provide data security. Any user with the appropriate rights to data using a PC with a browser anywhere would be able to access the repository and search it using whatever performance utilities are in that solution.

3.3.2 Small Operation Back-end Solution

Small Operations with only one or a few trucks recover HOS records, just not as many as a Large Operation. This reduces the solution's complexity; it only needs to recover HOS data in a much smaller and less expensive database. The data is both pre-loaded and recovered from the same PC, probably at the Owner-Operators base of operations. The solution could reside on a single PC with a GUI-driven application that both pre-loads and recovers the data to/from their Front-end solution. The application would also be able to search the HOS historical data and create reports, etc. The standard Windows Operating System with MS Access database could be used to minimize cost.



3.3.3 Owner-Operator Solution

Single Owner-Operators could use an integrated solution that combines the Front- and Back-end functions in a single device. There is no pre-loading or data transfer as the functions are incorporated in a single device. This could encompass the PDA, Windows CE, and PC classes of hardware but is probably too complex for a firmware solution.

The device would be docked when in-vehicle. At each status change the driver would input the appropriate status and the firmware device would gather the GPS and ECU data as needed, forming the HOS record which is then securely stored. After the trip the storage device is turned in and interfaced to a Back-end component with a reader that archives the records. In Large Operations the data would be moved directly to the repository.

If there is no GPS in the vehicle, a fixed database would allow the driver to rapidly pick from drop-down menus first for the state, then road type (interstate, federal road, etc.), road number to indicate the location. The nearest Place Name could also be recovered from the database providing all the required information in the HOS records for the trip. Some provision should be made in these solutions to backup the data after each trip, either in additional storage media, or with printouts, to meet the 6-month retention requirement.



High-Level Architectures for HOS Solutions

SECTION 4 - RECOMMENDATIONS

The following recommendations are related to the notional HOS architecture.

Use a common data record structure and minimum security requirements throughout the Front- and Back-end solutions. This will allow different vendor's solutions to be interchangeable and drive the marketplace to optimum performance and cost effectiveness.

Define three overall modes of operation for the Back-end Solutions: One for Large Operations with centralized data storage and networked terminals, another scaled down version of the same for Small Operations with a single data repository and terminal, and a third for single Owner-Operators with a single vehicle that uses an all-in-one single device for both the Front- and Back-end functions.

Specify industry standard development tools and techniques for solution construction. This will yield a common set of software products that can run on different hardware classes

Use the existing paper system (FMCSA Regulation, Section 395.8) to handle automated HOS solution failures in the field.

Inspectors should continue to use their existing enforcement procedures. All the in-vehicle HOS solutions will have a compliance function that will visually inform the inspector and driver of any problems. This will allow the inspectors to check compliance without having to be trained on the numerous HOS Front-end solutions that will be available in the future.



BIBLIOGRAPHY

The 6 documents used in the research are listed below and on the next page. Portable Document Format (PDF) and MS Word are used. The entire listing is included on the CD-ROM for this module.

#	Title
1	HOS Data Specification Module
2	ECM TCM Usage for HOS Solutions Module
3	Geo-Referenced Data in HOS Solutions Module
4	HOS Paper Backup System Module
5	Notional Place Name Book Example - VA
6	Notional State Border Crossing Book Example - VA