



February 2002

**SAE J1760**

**ITS Data Bus (IDB) Data Security Services Recommended Practice**

**Overview**

The ITS Data Bus (IDB) is a common network interface for consumer devices in vehicles. A serial communication bus, it may be the bridge between the development-cycle time difference of automobiles and electronics. It may also meet the need to be able to upgrade automobile electronics during the life of the vehicle.

The long development time required to produce a new automobile and the short development time of today's consumer electronic devices has meant that the electronics in a vehicle might lag the state of the art by several years. With the growing consumer-oriented electronics content in today's vehicles, it is becoming more difficult for the automotive manufacturers to meet consumers' expectations for electronic devices in vehicles. The result is increasing pressure on the vehicle manufacturers from after-market electronics suppliers, who can update and expand their product lines quickly.

The advent of an open-standards data bus, such as the IDB, with its access to vehicle functions, necessitates concerns about data security and privacy. This recommended practice describes the data security services for the IDB by defining data security requirements between devices and by defining device- and message-level security. It also describes a mechanism to discourage theft of data bus devices.

**What is this standard for?**

The IDB (described in the SAE J2366 ITS Data Bus series of standards documents) is an open, non-proprietary serial communication protocol designed to allow a wide variety of consumer devices to share information across a common network in a vehicle. To add system functionality, the IDB can be interfaced to the existing OEM vehicle bus via a "gateway" (described in SAE J2367 - ITS Data Bus Gateway Recommended Practice), which allows a selective exchange of data between devices on the IDB and devices on the vehicle bus. This allows the IDB to operate independently of all vehicle systems, giving the consumer electronics manufacturers the freedom to integrate IDB interfaces into their popular consumer products without the need for performing a full automotive-level network qualification.

Given the current trend towards extensive communications in and out of a vehicle, it becomes even more important that data exchanges among or between IDB devices and vehicle systems be protected. Remote access to vehicle functions (especially those that are safety related such as braking) must be controlled, authorized, and tracked. Protection must be provided against "spoofing" (inserting false or erroneous information or data into a communications stream or computer in order to cause it to provide an erroneous output), and data "sniffing" (an unauthorized user or person's attempt to read the information being transferred to a computer). These protection mechanisms must also be in place for devices installed into vehicles, since access to vehicle functions could be obtained via relatively easily installed devices.

This standard, **SAE J1760 - ITS Data Bus (IDB) Data Security Services Recommended Practice**, defines a method for providing data security for the IDB without diminishing any of the benefits of the IDB interface. An example of this can be found in Internet technology where encryption ensures data security within a standards environment.

**Who uses it?**

This recommended practice is intended for use by vehicle manufacturers (including electronic and platform engineers and designers) and suppliers and manufacturers of vehicle consumer electronics products. These users will find a range of operating rules in the standard for developing and improving their products and systems with respect to security. By following

To obtain a copy of this standard, please contact:

**Society of Automotive Engineers (SAE)**  
400 Commonwealth Drive  
Warrendale, PA 15096  
Tel: (724) 776-4841  
Fax: (724) 776-0243  
Web site: [www.sae.org](http://www.sae.org)

Publication Date: December 2001

this standard, they will be able to ensure that their products are compatible and that they will be able to take full advantage of more complex data sources without loss of compatibility.

#### **How is it used?**

This recommended practice defines the security methods to be used so that all IDB-conformant devices can be integrated and can interoperate. Its use will assure that IDB-conformant devices can communicate with appropriate vehicle systems for maximum effectiveness.

#### **Scope**

The specification covers the various aspects of data security including, but not limited to, authorization and authentication.

#### **Related documents**

To accommodate the broad scope of this effort, the IDB specifications have been divided into several individual documents. At present, the following documents are defined:

#### **SAE J1760—ITS Data Bus Data Security Services Recommended Practice (this standard)**

[SAE J2355—ITS Data Bus—Architecture Reference Model Information Report](#)

[SAE J2366-1—ITS Data Bus—Protocol Physical Layer Recommended Practice](#)

[SAE J2366-2—ITS Data Bus—Protocol Link Layer Recommended Practice](#)

[SAE J2366-4—ITS Data Bus—Protocol Thin Transport Layer Recommended Practice](#)

[SAE J2366-7—ITS Data Bus—Protocol Application Message Layer Recommended Practice](#)

[SAE J2367—ITS Data Bus—Gateway Recommended Practice](#)

[SAE J2590—PMODE for In-Vehicle Networks Recommended Practice](#)