represent good treadle design, it does not intrinsically overcome a disconnection anywhere within an electronic accelerator control system. Thus, good treadle design does not provide an electronic accelerator control system with the same degree of fail-safe operation provided a mechanical system by redundant return springs on a traditional fuel control rack. Those springs on a traditional rack could overcome an accelerator control disconnection and return the throttle to idle. Further, providing good treadle design does not solve the problem of single point disconnection in electronic systems which now would include connectors, wires, computer components and possibly even software elements. Even parties recognizing the analogy between wire severance and linkage severance have asked whether the standard applies to subsequent short circuits as well as open disconnections.

NHTSA believes that the volume of requests for interpretation might be reduced if, instead of answering these questions by drawing analogies between traditional mechanical components and new electronic systems, it amended the Standard to include provisions and language specifically tailored to electronic systems. There are limitations to the agency's ability to make regulatory language, which reflects the design of mechanical systems, serve the purpose of regulating both mechanical and electronic systems. NHTSA also believes that amending the Standard not only to update it, but also possibly to redefine what constitutes fail safe operation might give manufacturers more flexibility in designing electronic systems and enable the agency to better ensure that electronic systems function safely. In order to do this, the agency must identify the most common predictable failures for electronic systems and ascertain the most appropriate response to those failures.

NHTSA is also concerned that regulating electronic systems by drawing analogies to mechanical systems may have the effect of limiting the permissible responses to failures in electronic systems to the fail-safe modes of mechanical systems. At present, the failure modes (i.e., disconnection and severance) specified in Standard No. 124 are the predictable failure modes of a mechanical system. The agency believes that the regulation of electronic systems in a manner tailored to them can be beneficial to manufacturers, vehicle users, and the public. For example, with electronic systems, there may be failure modes in which it is wiser to either shut down the engine or to provide for a fail-safe mode in which the engine has just enough power to permit the vehicle to be driven to the side of the road, than to require that the engine be returned to idle. Since such choices were not feasible with mechanical controls, they were not included in Standard No. 124.

Through this request for comments, NHTSA wishes to determine whether it can propose amendments which identify the predictable failure modes of electronic systems and specify an acceptable safe response for each mode.

Normal v. Failure Modes

On many trucks, locking hand controls are necessary for the operation of engine-driven vocational equipment, i.e., work-performing equipment such as garbage compactors or cement mixers, when the vehicle is parked. Similar locking hand controls are also provided to facilitate engine warm-up. Obviously, locking hand controls can be thought of as preventing the return to normal idle speed when the accelerator pedal is released (defined in the Standard as a failure). Several requests for interpretation have resulted. However, locking hand controls do not affect highway safety because the locking controls are not meant to be used to drive vehicles. Explicit specification in the standard of what is or is not permissible with respect to the operation of locking hand controls could eliminate a source of ambiguity.

Likewise, the lack of absolute repeatability in the normal operation of some electronic accelerator controls results in the return to a range of idle speeds instead of a single idle speed. While this range is narrow enough to permit safe operation of a vehicle, the return to a range of speeds instead of a single speed nevertheless introduces questions about whether a range is narrow enough to be regarded as complying with the requirements of the standard for return to idle speed. A revision of the standard offers an opportunity to adopt language that distinguishes between normal safe characteristics of accelerator controls and instances of failure.

Questions for Comment

In order to determine whether the agency should propose to amend Standard No. 124 and to obtain a better idea of technology that is presently available, NHTSA asks the following questions to clarify engineering issues. Sections A and B apply to electronic systems only. Sections C, D, E and F are of general applicability.

A. Industry Consensus

The Society of Automotive Engineers (SAE) has developed recommended practices for electronic signal interfaces for heavy diesel vehicle engine control processors and for some aspects of accelerator pedal position sensor performance. The SAE's recommended practice specifies that the accelerator position sensor (APS) assembly shall comply with all appropriate Federal motor vehicle safety standards.

A1. Has the SAE or other industry consensus standards organizations considered fail-safe provisions for electronic accelerator controls? Is there industry agreement (informal or formal) concerning what fail-safe provisions should be adopted for electronic accelerator control systems?

A2. What fail-safe strategies are now being employed by vehicle and component manufacturers?

B. Technical Considerations of a Fail-Safe Electronic Accelerator Control System

NHTSA believes that the potential points of failure of an electronic accelerator control system are:

—the mechanical linkage and return springs between the pedal and the accelerator position sensor (APS);
—the electrical connections between the APS and the engine control processor;
—the electrical connections between the engine control processor and other critical sensors;
—the electrical connections between the engine control processor and fuel or air metering devices which determine engine speed;
—power to the engine control processor, the APS and critical sensors; and
—the integrity of the engine control processor, APS, and other critical sensors.

A single point disconnection would mean the severance of a single wire or the disconnection of all the terminals housed in a single connector. The consequences both of an open circuit or a short circuit would ordinarily be relevant, but NHTSA does not exclude the possibility that some designs could prevent either a short circuit or an open circuit in the event of a disconnection. Critical sensors are those whose malfunction or disconnection could cause a significant uncontrolled engine overspeed. The agency is not aware that sensors other than the APS are critical in a safety sense.

With this background, NHTSA asks the following questions:

B1. Are there other predictable points of failure of an electronic control system?