U.S. Department
of Transportation
**National Highway
Traffic Safety
Administration**

People Saving People
http://www.nhtsa.dot.gov

PB99-113896

DOT HS 808 803

September 1998

Final Report

Technology Review for Electronically Controlled Braking Systems

Technical Report Documentation Page

1. Report No.	2.	3. Recipient's Catalog No.
DOT HS 808 803	PB99-113896	

4. Title and Subtitle	5. Report Date
Technology Review for Electronically Controlled Braking Systems	September 22, 1998
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Grace, R., Wiss, J. W., Hudak, J. J., and Eubanks, C.N. *	

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Carnegie Mellon Driving Research Center 700 Technology Drive Pittsburgh, PA 15230-2950	11. Contract or Grant No. DTNH22-93-D-07007

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
DOT/National Highway Traffic Safety Administration 400 Seventh Street, S.W. Washington, D.C. 20590	Final Report
	14. Sponsoring Agency Code

15. Supplementary Notes - Additional Contributors

*Motor & Equipment Manufacturers Association
10 Laboratory Drive
Research Triangle Park, NC 27709-3966

*SAE Truck and Bus Council - Future Brake Systems Forum (SAE-EBS Task Force)
Society of Automotive Engineers
400 Commonwealth Drive
Warrendale, PA 15096-0001

16. Abstract

Electronically Controlled Braking Systems (ECBS) offer many potential benefits to the trucking industry in the areas of safety, reliability, enhanced driver feedback, and maintainability. ECBS are being tested by a number of manufacturers. These systems are intended to replace the current pneumatic brake application signal with an electronic actuation signal. This report represents a preliminary review of ECBS technology. The stakeholders considered in this report are the users (operating truck fleets), the truck manufacturers, the brake manufacturers, and the federal government.

The ultimate customers, the fleets, are key to the successful introduction of ECBS. The fleets see ECBS as a promising technology and natural evolution of the success of electronically controlled engines and transmissions. The major concern of the federal government is safety. The National Highway Traffic Safety Administration (NHTSA) interest are to create a practical performance standard for ECBS or to provide information to establish industry recommended practices. These performance standards should provide a minimum standard for stopping capabilities and safety assurance (fail-safe performance). The major issue facing NHTSA is whether to modify federal motor vehicle standard No. 121, to include ECBS, or to produce a new regulation that directly addresses the issues of ECBS.

The identified barriers to the deployment of ECBS are: the potential increased cost of ECBS; lack of data on ECBS promised benefits; lack of industrial standards regarding ECBS; lack of human factors data regarding new ECBS features such as brake feel; lack of federal regulations; system security - assuring that information available on the communications buss remains proprietary.

17. Key Words		18. Distribution Statement
Pneumatic Braking	Electronically Controlled Braking Systems	Document is available to the U.S. public through the National Technical Information Service, Springfield, VA 22161
Safety	Reliability	
Performance Standards	Communications architecture	
Fail-safe	Communications Protocol	
Software	Compatibility	
Critical Systems		

19. Security Classif. (of this report)	20 Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified		

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY 1

2 INTRODUCTION 3

2.1 BRIEF REVIEW OF PNEUMATIC BRAKING TECHNOLOGIES 4

3 STAKE HOLDERS' ISSUES 5

3.1 FLEETS (CUSTOMERS) 5
3.2 TRUCK MANUFACTURERS 6
3.3 BRAKE MANUFACTURERS 7
3.4 FEDERAL GOVERNMENT 7

4 IDENTIFIED BARRIERS TO COMMERCIAL INTRODUCTION 8

5 COMMUNICATIONS PROTOCOLS 10

6 FAIL-SAFE ANALYSIS 16

6.1 SAFETY AND RELIABILITY 16
6.2 SOFTWARE SAFETY AND RELIABILITY 17
6.2.1 Fault-Tolerant Software Engineering 17
6.2.2 Software System Analysis 19
6.3 FAIL-SAFE ANALYSIS FOR DISTRIBUTED CONTROL SYSTEMS 19

7 COMPATIBILITY ISSUES 22

7.1 ECBS CLASSIFICATIONS AND CONFIGURATIONS 22
7.2 COMPATIBILITY WITH PNEUMATIC/ABS SYSTEMS 26
7.3 COMPATIBILITY AMONG BRAKE MANUFACTURERS 28
7.3.1 Tractor/Trailer Compatibility 28
7.3.2 Component Level Compatibility 30

8 SENSORS FOR DIAGNOSTICS AND IMPROVED BRAKING PERFORMANCE 31

8.1 BRAKE DIAGNOSTIC SENSORS 31
8.2 DIAGNOSTIC TOOLS 33
8.3 SENSORS FOR ENHANCED BRAKING CAPABILITIES 34

9 REGULATORY ISSUES 35

9.1 REGULATORY ISSUES AND STAKEHOLDER COMMENTS 35
9.2 POSSIBLE CHANGES FMVSS NO. 121 36
9.3 AAR SPECIFICATIONS FOR ELECTRONIC BRAKING SYSTEM FOR FREIGHT TRAINS 37
9.4 DESIGN NEUTRAL PERFORMANCE BASED REGULATION 38
9.4.1 FAA Regulatory Model 39
9.5 CLOSING REMARKS 41

10 9 RECOMMENDATION FOR FURTHER STUDY 41

10.1 TRACK TESTS 41
10.2 TECHNICAL REVIEW OF CRITICAL SOFTWARE DEVELOPMENT PROCESSES 42

11 REFERENCES 44

A1 PROPOSED CHANGES TO FMVSS NO. 121 ..... A-1

A2 AAR SPECIFICATION S-4200 ..... A-8

A3 AAR SPECIFICATION S-4210 ..... A-27

A4 AAR SPECIFICATION S-4220 ..... A-49

A5 AAR SPECIFICATION S-4230 ..... A-56

A6 FAA REGULATIONS A-100

A7 EUROPEAN REGULATIONS A-104

1 EXECUTIVE SUMMARY

Pneumatic truck brakes use air as a medium for transmitting pressure from a driver control to the service brake. The modern pneumatic braking system is a split air system which consists of two separate air circuits. The primary brake circuit typically controls the brakes on the rear drive axles and the trailer. The secondary brake circuit typically controls the air on the front steering axle and can also be used to control the trailer brakes. If a failure occurs in either circuit, the pressure is contained and partial braking capability is maintained for a limited number of brake actuations.

Electronically Controlled Braking Systems (ECBS) is the next technology step in the evolution of pneumatic brakes. With ECBS the actuation of the pneumatic brakes is done through electronic messaging and active computer control, but the stopping power remains air pressure. When the driver depresses the brake pedal an electronic control unit (ECU) detects the position of the brake pedal and transmits a corresponding braking signal to one or more brake control ECU's. The brake control ECU's then adjust the brake pressure or stopping torque to the commanded value. With ECBS brake actuation time is significantly reduced and costly plumbing in the tractor is reduced.

ECBS offer many potential benefits to the trucking industry in the areas of safety, reliability, enhanced driver feedback, and maintainability. ECBS are being tested by a number of manufacturers. These systems are intended to replace the current pneumatic brake application signal with an electronic actuation signal. This report represents a preliminary review of ECBS technology. Its objectives are to identify the potential benefits of ECBS, to identify the barriers to commercial introduction and to develop a rational test plan to support the introduction of ECBS.

The stakeholders considered in this report are the commercial truck fleets, the truck manufacturers, the brake manufacturers and the federal government. The ultimate customers, the fleets, are key to the successful introduction of ECBS. The fleets see ECBS as a promising technology and a natural evolution of the success of electronic engines and transmissions.

The truck manufacturer's role is primarily one of systems integration. They are responsible for the installation of systems obtained from the various ECBS manufacturers. They are also responsible for meeting government safety regulations and for assuring that ECBS work safely, reliably and effectively with other systems on the vehicle. To accomplish this they will need to work closely with other stakeholders to define a safe, reliable and effective communications architecture.

Brake manufacturers are primarily responsible for the safety, reliability and effectiveness of their ECBS products. They are responsible for designing and manufacturing systems that meet the requirements of their customers (the fleets and truck manufacturers). They are also responsible for the fail-safe performance of the internal system features including all pneumatic, electronic and software components. The brake manufacturers will, of course, play a major role in developing standards for compatibility of ECBS among manufacturers. The brake manufacturers will also have a hand in the design of the communications architecture and the development of standards for compatibility between tractors and trailers

The major concern of the federal government is safety. The National Highway Traffic Safety Administration (NHTSA) is eventually responsible for developing the safety standards. NHTSA's interests are to create a practical performance standard for ECBS or to provide information to establish industry recommended practices. These performance standards should provide a minimum standard for stopping capabilities and safety assurance (fail-safe performance). The

major issue facing NHTSA is whether to modify federal motor vehicle safety standard FMVSS No.121, to include ECBS, or to produce a new regulation that directly addresses the issues of ECBS.

The Federal Highway Administration (FHWA) also plays a role in ECBS standards. As the body that is responsible for the safe operation of motor vehicles used in interstate commerce, FHWA is interested in developing inspection standards that are both thorough and efficient. ECBS, if designed properly, could allow inspectors to evaluate the status of the braking system through electronic communications methods.

The identified barriers to the deployment of ECBS are: the potential increased cost of ECBS; lack of data on ECBS promised benefits; lack of industrial standards regarding ECBS; lack of human factors data regarding new ECBS features such as brake feel; lack of federal regulations; system security – assuring that information available on the communications bus remains proprietary.

An essential part of ECBS is a safe, reliable and effective communications protocol. Three communications protocols applicable to ECBS are presented and compared. The standards considered here are: 1) SAE J1939 which is the most likely candidate for use with ECBS; 2) Echelon/LonWorks which is currently being applied to electronic braking for freight trains; and 3) TTP (time triggered protocol) which is a new protocol claiming to have features that will improve the ability to analyze the safety and reliability of distributed control systems. These network protocols are based on standards produced by the International Standard Organization (ISO) for open system interchange (OSI) known as the ISO-OSI 7-Layer Reference Model.

Safety and reliability of ECBS are key issues. ECBS as a safety critical system must not fail or fail-safe (i.e. allow the vehicle to stop safely after a failure occurs). Addressing these issues requires a discussion of safety and reliability issues for both software and communications components of ECBS. Because of the inherent complexity of both software and communication systems, it is impossible to assure safety. However, tools and methods have been developed for both system design and system evaluation that have been shown to produce safe and reliable systems.

Compatibility is also an important issue for ECBS. Since ECBS will likely be phased in over many years, it is important that ECBS equipped tractors (trailers) be compatible with today's pneumatic/ABS equipped trailers (tractors). It is also desirable to have compatibility among manufacturers. Tractor-trailer compatibility for different manufacturers requires a common and open communications architecture. Component level compatibility, which requires a much more detailed standardization process, is desired by the fleets. However, brake manufacturers may wish to differentiate their product at the component level.

ECBS and its associated communications protocol will provide a basis for the addition of sensors for both diagnostic purposes and to improve the braking process, potentially decreasing stopping distances and improving the stability of the vehicle.

The deployment of ECBS will require a review and modification of existing braking regulations. Three approaches for this are provided in this report. The first approach considers minimal changes to the existing FMVSS No.121. Although this approach is expedient, it does not address the important issues regarding software safety and reliability. The second approach looks to the railroad industry where detailed specifications are being developed for electronic brakes. The railroad approach is specific to a particular communications protocol and spells out in great detail how safety and reliability are to be achieved. The drawback to this approach is that it is rigid and requires industry consensus for innovation to occur. The third approach looks to the aviation

industry for a true performance based / design neutral approach. The drawback to this approach is compliance. Compliance will likely require a significant paper trail from the brake manufacturers, the truck manufacturers and the fleets (maintenance, etc.)

In conclusion, it is recommended that a program proceed as soon as possible to quantify the benefits of ECBS. The logical starting place for this endeavor is at the test track. Through track tests the improved braking performance of ECBS can be clearly demonstrated when compared to today's pneumatic/ABS brakes.

It is also recommended that a program to technically review software development processes as applied to safety critical systems be considered by NHTSA This information will provide NHTSA and the industry as a whole with the knowledge base needed to both evaluate and regulate these new software based safety critical systems.

2 INTRODUCTION

Electronically Controlled Braking Systems (ECBS) are being tested by a number of manufacturers. These systems are intended to replace the current pneumatic brake application signal with an electronic actuation signal. ECBS offer many potential benefits to the trucking industry in the areas of safety, reliability, enhanced driver feedback, and maintainability. The potential benefits include:

- shorter stopping distance,
- improved traction control,
- load adjustable deceleration control,
- brake fade sensing and compensation,
- reduced brake actuation time,
- more sophisticated system and component diagnostics,
- improved brake wear,
- reduced maintenance costs.

ECBS with a pneumatic backup system are currently being evaluated on tractors and trailers. These systems represent the first effort to deploy commercial ECBS in the U. S. However, for the benefits of ECBS to be fully realized, a number of obstacles must be overcome. First, tractor and trailer ECBS must be shown to be safe and effective. Only when all wheels are equipped with ECBS, can smart braking strategies be employed that can provide safer stopping with improved stability. In addition, concerns regarding safety, reliability, durability, initial cost and maintenance costs of ECBS must be demonstrated and quantified. For fleets to accept ECBS, steps must be taken to demonstrate that they are safe and reliable. ECBS must also be affordable, easy to trouble-shoot, repairable at a reasonable cost, and not require extensive retraining of technicians.

This report represents a preliminary review of ECBS technology. Its objectives are to identify the potential benefits of ECBS, to identify the barriers to commercial introduction and to develop a rational test plan to support the introduction of ECBS. Information presented in this report was gathered from the literature and from discussions with various stakeholders.

2.1 BRIEF REVIEW OF PNEUMATIC BRAKING TECHNOLOGIES

Pneumatic truck brakes use air as a medium for transmitting pressure from a driver control to the service brake. The modern pneumatic braking system is a split air system which consists of two separate air circuits. The primary brake circuit typically controls the brakes on the rear drive axles and the trailer. The secondary brake circuit typically controls the air on the front steering axle and can also be used to control the trailer brakes. If a failure occurs in either circuit, the pressure is contained and partial braking capability is maintained for a limited number of brake actuations.

The current heavy vehicle brake standards are pneumatic brakes with Antilock Braking Systems (ABS). As of March 1, 1997 all new tractors are to be equipped with ABS. As of March 1, 1998 all new trailers will be equipped with ABS. The purpose of ABS is to maintain maximum vehicle stability during extreme braking conditions.

The current implementation of ABS is the application of a computer controlled brake modulation system over top of conventional pneumatic brakes. The goal of the ABS is to maintain wheel slip at a point that provides a balance between braking traction and cornering traction. Maximum braking traction can occur at a wheel slip that corresponds to sharply reduce cornering traction. Hence, ABS is a compromise between braking and stability

ECBS is the next technology step in the evolution of pneumatic brakes. With ECBS the actuation of the pneumatic brakes is done through electronic messaging and active computer control, but the stopping power remains air pressure. When the driver depresses the brake pedal an electronic control unit (ECU) detects the position of the brake pedal and transmits a corresponding braking signal to one or more brake control ECU's. The brake control ECU's then adjust the brake pressure or stopping torque to the commanded value. With ECBS brake actuation time is significantly reduced and costly plumbing in the tractor is reduced.

As ECBS becomes accepted, additional sensors can be added to provide information necessary for additional ECBS specific features. For example, by implementing an axle load sensor, the braking pressure for each axle can be load-adjusted for more even braking. Feedback can be provided to give the driver a brake feel similar to that of hydraulic brakes. Temperature sensors or torque sensors may also be incorporated to enhance the ability to diagnose system performance and to take steps to avoid catastrophic and costly incidents. The addition of active suspension used together with ECBS is the basis for vehicle dynamic control (Ref. 1, 2). Eventually sophisticated collision avoidance systems will use ECBS as a means for controlling the brakes to help avoid crashes.

Currently ECBS is offered in the U. S. on tractors only with dual redundant pneumatic backup systems. A dual redundant pneumatic backup system employs two independent pneumatic circuits consistent with FMVSS 121. The next step in the evolution of ECBS will be to extend ECBS to the trailer. In the following evolutionary steps, the cost of the system can be reduced by the introduction of ECBS with a single pneumatic backup system. This will reduce the cost and complexity of the pneumatic system while maintaining compatibility with standard pneumatic systems. The final evolutionary step might be to develop a redundant ECBS with no pneumatic backup. A redundant ECBS system contains two independent ECBS control systems but no pneumatic backup system. Compatibility of the redundant ECBS tractor (trailer) with a pneumatic

trailer (tractor) can be accomplished by adding capability to convert the electronic(pneumatic) signals to a pneumatic (electronic) signal.

3 STAKE HOLDERS' ISSUES

3.1 FLEETS (CUSTOMERS)

The ultimate customers, the fleets, are key to the successful introduction of ECBS. The fleets see ECBS as a promising technology and a natural evolution of the success of electronic engines and transmissions.

The benefits of ECBS to the fleets include:

- *Improved stopping performance under all driving conditions.*

  This includes minimizing brake actuation time, reducing the potential for brake fade, and providing better brake balance.

- *Providing the driver and fleet manager with feedback and system status information.*

  Onboard system diagnostics have the potential to identify problems with the braking system in an early stage (before a brake failure occurs). This information can be presented to the driver, transmitted to the fleet manager and/or used as part of the roadside inspection process. Based on this information, appropriate decisions can be made with regard to corrective actions. This concept of just in time (JIT) maintenance has the potential of reducing maintenance costs and preventing potentially hazardous brake failures.

- *Expanding the uses of a common maintenance and diagnostic communications architecture.*

  The trend in the industry is to move towards computer-based diagnostic and maintenance systems. These systems offer a potential for rapidly inspecting, diagnosing and repairing onboard brake systems.

- *Reduction in brake shoe wear.*

  Conventional pneumatic brakes can provide uneven braking force leading to high temperatures for the brake shoes that are carrying the greater load. This situation leads to rapid acceleration of brake shoe wear due to the higher temperature, and may contribute to brake fade. Electronic control would, in principle, provide for even braking, sharply reducing the potential for these problems.

  In addition, the potential exists for the automatic coordination of the engine retarder systems with ECBS, further reducing brake shoe wear.

- *Rapid roadside inspection.*

  Onboard diagnostics could be used by the enforcement community as an alternative or supplement to manual brake inspection. This, in principle, can reduce the valuable time spent

for roadside brake inspection providing a significant productivity benefit to the fleets and the enforcement community.

- *Provide a basis for innovation.*

  The widespread application of ECBS would provide an onboard infrastructure needed to develop new important safety features. Electronic control would ease the introduction of disc brakes on the steering axle by providing a means to adjusting for the different pneumatic requirements of disc brakes. In addition, the introduction of active suspension used in conjunction with ECBS makes possible the application of vehicle dynamic control (VDC).

Fleets Concerns:

- The benefits as discussed above need to be clearly demonstrated and quantified.
- The impact on residual (trade-in) value must be explored and explained. Will the rapid evolution of electronics and software render a vehicle obsolete in a relatively short period of time?
- The durability and maintainability of the ECBS must be clearly demonstrated.
- Standards related to ECBS must be put in place including:
  - Communications architectures must be developed that insure interoperability among manufacturers and ensure the safety/reliability of the communications process.
  - Standards for interoperability between tractors (trailers) with ECBS and trailers (tractors) with conventional pneumatic/ABS brakes.
  - SAE J560 trailer/tractor connector.
  - Standards for ECBS diagnostic messages.
- Recommended maintenance practices must be put in place including:
  - Recommended procedures for use of computer-based diagnostic equipment.
  - Recommended procedures/actions for responding to onboard diagnostic messages.

3.2 TRUCK MANUFACTURERS

The truck manufacturer's role is primarily one of systems integration. They are responsible for the installation of systems obtained from the various ECBS manufacturers. They are also responsible for assuring that ECBS work safely, reliably and effectively with other systems on the vehicle. To accomplish this they will need to work closely with other stakeholders to define a safe, reliable and effective communications architecture.

The truck manufacturers, as the designers and implementers of the vehicles' communications

architecture, will be responsible for the various diagnostic interfaces for the driver, maintenance personnel, and enforcement personnel. Compatibility with tractor and trailer is also a major concern. They will coordinate with other stakeholders to assure tractor/trailer compatibility. The truck manufacturers will also have a hand in establishing standards for compatibility of ECBS among manufacturers. They are also responsible for implementing complex braking and collision avoidance strategies that will require the coordination of multiple systems on the vehicle.

3.3 BRAKE MANUFACTURERS

Brake manufacturers are primarily responsible for the safety, reliability and effectiveness of their ECBS products. They are responsible for specifying, designing and manufacturing systems that meet the requirements of their customers (the fleets and truck manufacturers). They are also responsible for the fail-safe performance of the internal system features including all pneumatic, electronic and software components.

The brake manufacturers will, of course, play a major role in developing standards for compatibility of ECBS among manufacturers. The brake manufacturers will also have a hand in the design of the communications architecture and the development of standards for compatibility between tractors and trailers

3.4 FEDERAL GOVERNMENT

The major concern of the federal government is safety. Congress passed the "National Traffic and Motor Vehicle Safety Act of 1966" (recodified as Chapter 301 of Title 49 U.S. Code) with the purpose of reducing accidents, and deaths and injuries resulting from traffic accidents. Part of that Act directed the Secretary of Transportation to establish motor vehicle safety standards for motor vehicles and equipment in interstate commerce. The Act defined "Motor Vehicle Safety Standards" to mean a minimum standard for motor vehicle performance, or motor vehicle equipment performance, which is practicable, which meets the needs for motor vehicle safety, and provides objective criteria.

The National Highway Traffic Safety Administration (NHTSA) is eventually responsible for developing the safety standards as defined above. According to this definition, NHTSA's interests would be to create a practical performance standard for ECBS or to provide information to establish industry recommended practices. These performance standards should provide a minimum standard for stopping capabilities and safety assurance (fail-safe performance). The major issue facing NHTSA is whether to modify federal motor vehicle safety standard (FMVSS)-121 to include ECBS or to produce a new regulation that directly addresses the issues of ECBS.

The Federal Highway Administration (FHWA) also plays a role in ECBS standards. As the body that is responsible for the safe operation of motor vehicles used in interstate commerce, FHWA is interested in developing inspection standards that are both thorough and efficient. ECBS, if designed properly, could allow inspectors to evaluate the status of the braking system through communications methods.

4 IDENTIFIED BARRIERS TO COMMERCIAL INTRODUCTION

In this section we will define and briefly discuss the identified barriers to commercial introduction of ECBS. The identified issues will be discussed in detail in the following sections:

- Cost.

  Trucking is a highly competitive industry with very small profit margins. Hence, for ECBS to be accepted by the fleets it must be cost effective. If cost of ECBS is greater than that of current braking systems, then the increased costs will need to be balanced with a corresponding increase in productivity and/or improved safety. In addition, fleets are concerned about the impact ECBS will have on the residual value of used vehicles related to the obsolescence of the rapidly evolving electronics and software.

- Lack of data on ECBS.

  Although the benefits of ECBS are appealing, the industry remains skeptical with regard to realization of these promises. In addition, considerable disagreement is present in the industry with regard to the nature and magnitude of the benefits. These issues can only be resolved by collecting data over time and quantifying the safety, productivity, and reliability benefits.

- Lack of standardization.

  Standards play an important role in the process of introducing ECBS. A number of important standards must be put in place before ECBS can be widely accepted. Some of the standards processes have begun and others are yet to be initiated. Standards issues include:

  - Compatibility of systems across manufacturers.
  - Compatibility of new ECBS equipped tractors (trailers) and current pneumatic/ABS trailers (tractors).
  - Complete definition and standardization of the in-vehicle and off-vehicle communications protocols.
  - Specification for storage and acquisition of diagnostic and inspection information.

- Lack of human factors data.

  Proposed ECBS products include potential improvements in the driver interface and possible automatic intervention for potentially hazardous situations. Features being discussed include the incorporation of a brake feel, presenting the driver with diagnostic and fault indicators, providing the driver with suggested actions to be taken depending on the severity of the fault, and automatic interventions such as "limit mode" that limit the driver's actions.

  Careful study of these proposed driver interface features and automatic intervention features is important from both acceptance and safety points of view. Questions to be asked include:

  - Is the "brake feel" appropriate and useful to the driver?
  - Are the fault indicators easily identified and interpreted by drivers, technicians and inspection officials?
  - Are the suggested actions provided by the system appropriate under all circumstances?

- When should the driver override the suggested action?
- Are the automatic features such as "limp mode" safe under all conditions?
- Will the driver be given the ability to override the automatic features?

- Federal regulations.

  Federal regulations currently do not prohibit ECBS, provided there exists a pneumatic backup system in compliance with FMVSS No. 121. Regulatory changes will be necessary for ECBS introduction. However, there is little consensus within the industry as to how to proceed in developing new regulations. Suggested directions for incorporation of ECBS-based regulations include:

  - Modifying FMVSS 121 to include ECBS.

    A major concern with this approach is the specification of electronic and software safety. It is difficult to develop a regulation that will assure safety and reliability of proprietary electronics and software.

  - Developing new performance-based regulations.

    All segments of the trucking industry are seeking new government regulations that are design neutral (non prescriptive). The goal is to establish new regulations that will assure the safety and reliability of braking systems while not limiting the innovation required to advance both braking systems and associated safety systems.

- Coordination with European regulations.

  Many brake and truck manufacturers have strong links to Europe. These links include cooperation with European counterparts, and in many cases American truck manufacturers are partially or fully owned by European companies. These strong links have led to efforts within the industry to standardize products resulting in better cooperation and lower cost to the customer. However, the brake designs and the regulator environments in these two communities are very different. The European regulation (ECE 324-R13) is less design restrictive than FMVSS No. 121. This results in a wider variation in braking system designs among manufacturers. The approval process is very demanding and costly. An extensive set of design reviews and system tests must be conducted in conjunction with a European governmental authority. Any effort to develop a truly universal brake design and regulatory system will be challenging.

- System security.

  ECBS will include capability of exchanging system information through both wired and wireless interfaces. The information available from the system could include:

  - Diagnostic information intended for use by technicians.
  - Inspection information intended for use by the enforcement community.

- Management information intended for use by fleet management.
- Warranty and liability information for use by the manufacturer.

In addition, it is possible that programmable ECBS features be included in some products. This information would presumably be accessed through the above-mentioned communications means. These features could be used to optimize, or otherwise alter, the system's characteristics for the particular driving circumstances.

Unauthorized access in any of the above situations is problematic. It is important that enforcement officials and technicians have access only to the information needed. It is vital that unauthorized personnel not be allowed to alter the programming of the system possibly reducing braking effectiveness and system safety. To accomplish this, network security procedures must be implemented within the selected network architecture.

5 COMMUNICATIONS PROTOCOLS

In this section three communications protocols applicable to ECBS will be presented and compared. The standards considered here are SAE J1939, Echelon/LonWorks and TTP (time triggered protocol). These modern computer networks are designed in a highly structured way. To reduce their design complexity, most networks are organized as a series of layers, each one built upon its predecessor. These network protocols are based on standards produced by the International Standard Organization (ISO) for open system interchange (OSI) known as the ISO-OSI 7-Layer Reference Model (Ref. 3).

The seven OSI layers are defined below:

1) Application Layer

The application layer contains a variety of protocols that are commonly needed. In control networks the application layer is responsible for message formats, machine independent signal characterization, and specifying parameter ranges. For example, there are hundreds of incompatible terminal types in the world. Consider the plight of a full screen editor that is supposed to work over a network with many different terminal types, each with different screen layouts, escape sequences for inserting and deleting text, moving the cursor, etc.

One way to solve this problem is to define an abstract network virtual terminal for which editors and other programs can be written. To handle each terminal type, a piece of software must be written to map the functions of the network virtual terminal onto the real terminal. For example, when the editor moves the virtual terminal's cursor to the upper left-hand corner of the screen, this software must issue the proper command sequence to the real terminal to get its cursor there, too. All the virtual terminal software is in the application layer.

Another application layer function is file transfer. Different file systems have different file naming conventions, different ways of representing text lines, and so on. Transferring a file between two different systems requires handling these and other incompatibilities. This work, too, belongs to the application layer, as do electronic mail, remote job entry, directory lookup, and various other general-purpose and special-purpose facilities.

2) Presentation Layer

The presentation layer performs certain functions that are requested sufficiently often to warrant a general solution, rather than letting each user develop a unique solution. Unlike all the lower layers, which are just interested in moving bits reliably from here to there, the presentation layer is concerned with the syntax and semantics of the information transmitted.

A typical example of a presentation service is encoding data in a standard, agreed upon way. Most user programs do not exchange random binary bit strings. They exchange things such as sensor inputs in defined units and status information with each bit having a defined status indication for a component of a control application. The job of managing these abstract data structures and converting from the representation used inside the computer to the network standard representation is handled by the presentation layer.

The presentation layer is also concerned with other aspects of information representation. For example, security issues such as data encryption and authentication are part of the presentation layer.

3) Session Layer

The session layer allows users on different machines to establish sessions between them to exchange larger amounts of data for a specific purpose. A session might be used to allow a user to connect a diagnostic device to the network and to transfer a diagnostic information file from one or more nodes*. If a large amount of information is being sent, the session layer can also allow for connection recovery if an error occurs during the file transfer.

4) Transport Layer

The basic function of the transport layer is to accept data from the session layer, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. The function of the transport layer is to isolate the session layer from the inevitable changes in the hardware. Under normal conditions, the transport layer creates a distinct network connection for each transport connection required by the session layer.

The transport layer also determines what type of service to provide to the session layer, and ultimately the users of the network. Transport layer functions include end-to-end acknowledgments, packet sequencing, and duplicate message detection.

5) Network: Routes the information in the network

The network layer is concerned with controlling the operation of the network. A key design issue is determining how packets are routed from source to destination. Routes could be based on static tables that are "wired into" the network and rarely changed. They could also be determined at the start of each conversation; for example, a diagnostic terminal session.

---

* A node is any device that sends and/or receives information across the network.

6) Data Link Layer

The main task of the data link layer is to take a raw transmission facility and transform it into a line that appears free of transmission errors in the network layer. It accomplishes this task by having the sender break the input data up into data frames (typically less than a few hundred bytes), transmit the frames sequentially, and process the acknowledgment frames sent back by the receiver. Since the physical layer merely accepts and transmits a stream of bits without any regard to meaning of structure, it is up to the data link layer to create and recognize frame boundaries. This can be accomplished by attaching special bit patterns to the beginning and end of the frame. If there is a chance that these bit patterns might occur in the data, special care must be taken to avoid confusion. The data link layer also provides error control between adjacent nodes.

7) Physical Layer

The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit. Typical questions here are how many volts should be used to represent a 1 and how many for a 0, how many microseconds a bit lasts, whether transmission may proceed simultaneously in both directions, how the initial connection is established and how it is torn down when both sides are finished, and how many pins the network connector has and what each pin is used for. The design issues here deal largely with mechanical, electrical, and procedural interfaces, and the physical transmission medium, which lies below the physical layer. Physical layer design can properly be considered to be within the domain of the electrical engineer.

SAE J1939

Of these three protocols. SAE J1939 is the clear leader for truck applications. Currently SAE J1939 is being employed for electronic engine and transmission control. SAE J1939 (Ref. 4, 5, 6, 7) is recommended practice (RP) for a "Class C" protocol based on Controller Area Network (CAN) 2.0 (Ref. 8). SAE J1939 is intended to be a true plug-and-play network; that is, the protocol is defined sufficiently to assure that any node developed by any manufacturer will function properly in the network providing the node complies with the published protocol specifications.

To accomplish plug-and-play capability involves defining all seven layers of the network protocol, and specifying a number of specific features of the control loops used in the vehicle. The approach taken by J1939 is to define all nodes and interconnections on the network. Hence for any "new" device to be added to a vehicle it must first be added to the system architecture.

The CAN protocol is targeted at high-speed, real-time control and can operate at up to 1 Mbyte/sec. CAN is based on the ISO 7 layer model, but defines only layers 1 and 2. Robert Bosch GmbH developed the CAN protocol in the early 1980s and worked with Intel on the first silicon implementation. This initial implementation of CAN version 1.2 (now known as version 2.0 part A) only allows for an 11-bit message identifier, thus limiting the number of distinct messages to 2032. In 1993 Intel released a new controller, the 82527, the first component to support the latest version of CAN version 2.0B. CAN 2.0B supports both the standard 11-bit and enhanced 29-bit identifier, allowing millions of distinct messages. CAN 2.0B is supported by a number of integrated circuit manufacturers.

CAN is a protocol for short messages. Each transmission can carry 0 - 8 bytes of data. This makes it suitable for transmission of trigger signals and measurement values needed for control applications. It is a CSMA/AMP (Carrier Sense Multiple Access / Arbitration by Message Priority) type of protocol. The protocol is message oriented and each message has a specific priority according to which it gains access to the bus* in case of simultaneous transmission.

An ongoing transmission is never interrupted. Any node that wants to transmit a message waits until the bus is free and then starts to send the identifier its message bit by bit. A zero is dominant over a one and a node has lost the arbitration when it has written a one but reads a zero on the bus. As soon as a node has lost the arbitration, it stops transmitting but continues reading the bus signals. When the bus is free again, the CAN Controller automatically makes a new attempt to transmit its message.

As the amount of data that can be sent in one transmission is limited to eight bytes, the maximum latency time of the highest priority message can be calculated. The maximum latency time of any message can be calculated if the nodes are restricted to the use of the same message identifier, once transmitted, until a specified time has elapsed. Every CAN Controller in a network will receive any message transmitted on the bus. Each node has to check whether a message is for it or not.

CAN was designed for event-driven systems, but it is not difficult to use the protocol in time-driven systems. Systems mixing both principles are also possible. The CAN Controller 72005 from NEC offers some features for time tagging of messages and for synchronization of local clocks at each node.

CAN features include:

- High data rates (1 Megabytes per sec (Mb/s) if the bus length is less than 40 meters).
- Non-destructive collision detection using bitwise arbitration.
- Specified message priority on the bus.
- The messages have a predictable maximum latency time. A trigger message with no data and the highest priority can have a maximum latency time of 54 microsecond (μs) on the bus if 1 Mb/s transfer rate is used.
- Messages can be sent point-to-point or be broadcasted or multicasted.
- Powerful error detection and handling is employed.
- Low-cost CAN Controllers and micro-controllers with built-in CAN Controllers are commercially available from Intel, Motorola, Philips, Siemens, and NEC.

---

* Bus is a general term used to describe the electrical medium used for communications. The most common bus in ECBS applications is a simple twisted-pair of wires.

Echelon/LonWorks

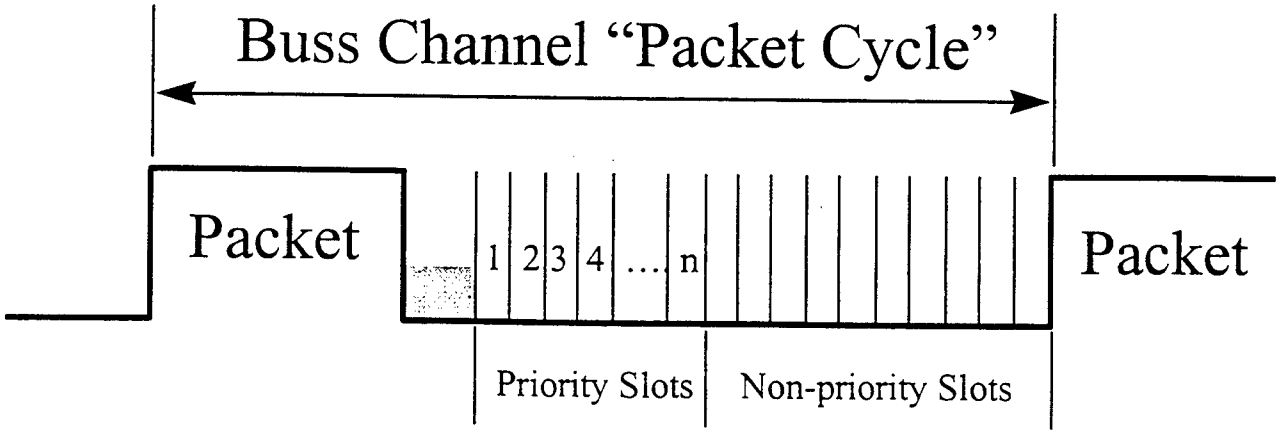
Echelon first introduced LonWorks in 1990 and worked with Motorola and Toshiba to develop the first silicon implementations (Neuron 312, 3150). Recently, Echelon has made arrangements to port the LonTalk protocol to user selected processors. LonWorks is currently being employed in a wide variety of applications in a number of industries.

The American Association of Railroads (AAR) has chosen LonWorks for the control of electronic brakes for freight trains. This implementation uses the Echelon PLT-10 power-line transceiver that transmits a signal on the power line.

LonWorks, like CAN, is a protocol for short messages. Maximum message size is 256 bytes. In practice, most messages carry only a few bytes. The main difference between CAN and Echelon is the bus access method. Bus access is accomplished through Non-Persistent CSMA (Non-Persistent Carrier Sense Multiple Access). The potential message latency for this technique is much higher than CAN, making it not as effective for real-time control applications needing response time in the few msec. range. Minimum latency on a LonWorks network is 7 msec. Typical latency is on the order of 50 msec.

As with CAN, an ongoing transmission is never interrupted. Any node that wants to transmit a message waits until the bus is free before it starts sending its message. Figure 1 is a graphical representation of the LonTalk bus access method. After the bus goes quiet, each node will delay its message transmission based on an assigned priority time slot or a randomly selected non-priority time slot. The first (n) time slots are used to send priority messages. Any priority 1 message will begin transmission during the first priority time slot. Any lower priority or non-priority message will not transmit until all priority 1 messages are transmitted. Only one node of a given priority can exist on a network.

Figure 1: **LonTalk Bus Access Method:** Once the bus becomes inactive, each node with a message to send will gain access based on a designated priority time slot or a randomly selected non-priority time slot.



Non-priority messages gain access to the bus based on the selection of a random delay time. If several non-priority messages are waiting to be sent, the node that selects the shortest random delay time will send its message while the others wait for the next quiet bus period.

Time Triggered Protocol

TTP has been specifically developed by Bosch AG for use in safety critical control environments. TTP is being considered for X-by-wire systems in passenger cars where X may be braking , steering or any other control system. The main difference between TTP and CAN or Echelon is the bus access feature. CAN and Echelon are event-driven protocols using CSMA bus access. That is, each node generates and receives messages in a conversational manner with minimal coordination with the other nodes on the network. If two or more nodes need to send a message, they compete for bus access using the rules of the bus access scheme. The approach used for TTP is to let each node transmit only in a selected time slot within a message cycle. Each node is assigned a time slot of length Δt to transmit a message. For a network of N nodes, each node must wait $N x \Delta t$ to transmit its next message. This eliminates the chance for collisions (assuming proper time synchronization) and provides a predictable latency for all messages.

The major advantage of TTP is that it simplifies the fail-safe analysis process for distributed control systems. The analysis of event-driven distributed control systems with all the associated timing parameters is very complex. With TTP, the analysis can be simplified and split into two parts:

1) Analyze each algorithm independent of network concerns.
   Standard techniques used in fail-safe analysis of software can be used for this part.

2) Verify the time-triggered aspects of the network.
   This is primarily insuring that the clocks on each node remain synchronized.

Drawbacks of TTP are:

- Latency for all messages grows as the number of nodes grows.
- A large fraction of a message cycle can be wasted if many do not choose to transmit one every message cycle.
- Is not immune to all network failure modes including the bus continuity and the babbling idiot node fault.

6 FAIL-SAFE ANALYSIS

It is a difficult process to determine the safety and reliability of a complex system involving electronics, software, and communications. Well established techniques are available for the evaluation of electronics reliability that have been used extensively by the military. The probability of any electronic failure can be directly calculated based on a mean time between failure estimate for each component in the circuit. Mean time between failure estimates are available for many military and industrial rated components.

Software reliability analysis processes are more complicated and less deterministic than those for electronics. The number of potential software failure modes is typically very large making a complete analysis impossible. However, a number of techniques have been successfully applied to fail-safe analysis of software (Ref. 9).

Communication reliability analysis processes, as applied to distributed control, can be looked at as an extension of software reliability. Only recently have the issues related to distributed control been considered as part of a formal analysis process (Ref. 10).

6.1 SAFETY AND RELIABILITY

It is very important to distinguish between safety and reliability. The reliability of a system can be defined as the probability that a system has full function in a time interval of a specified length, given that the system had full function at the start of the time interval. The safety of a system can be defined as the probability that a system does not fail in such a way that dangerous personal injuries or large economical losses can occur. As with reliability, safety can be defined as the probability that such critical failures do not occur in a time interval of a specified length, given that the system had full function at the start of the time interval.

A system can be very safe even if the system is unreliable. This is true if the system has a high probability of failing in a way that is not dangerous. Many systems can, without problems, be stopped when a safety critical failure is detected (fail silent mode). Other systems such as airplanes must remain operational after a fault occurs (fail operational mode). Current pneumatic braking systems are an example of a fail-silent system. If an error is detected in the primary braking system, emergency brakes are applied and the vehicle is stopped. Aircraft controls must remain operational during a flight. Hence, aircraft controls employ fail-safe operational systems.

In order to achieve a fail-safe behavior, it is required that the system is designed in such a way that it can either detect all failures that will lead to hazardous situations or that failures do not lead to hazardous situations. For the detection of such errors, some sort of redundancy normally is required. It is also required that the system can be forced to enter a safe state. For example, an open in a circuit might mean vital communications cannot be maintained. It is then required that the open circuit be detected, and that the system can be safely shut down or returned to a safe condition.

A system which is not developed with fail-safe behavior in mind will achieve that safety that is given by its failure rate. The problem with this is that the requirements for safety normally are much higher than the requirements for reliability. A typical figure for a hardware component is 1 failure in 10^5 hours and for a complete system, 1 failure in 10^4 hours. Such figures almost never meet safety demands.

6.2 SOFTWARE SAFETY AND RELIABILITY

Software reliability engineering is centered around a very important software attribute — reliability. Software reliability is defined as the probability of failure-free software operation for a specified period of time in a specified environment (Ref. 11). It is one of the attributes of software quality, a multi-dimensional property that includes other customer satisfaction factors including:

functionality, usability, performance, serviceability, capability, maintainability, and documentation (Ref. 12). Measurement of system failures is a key component in the quantification of reliability.

There is a significant difference in the way that software fails versus the way that hardware fails. Since software evolves through the first two stages of system development (specification & design, prototype) it is subject only to design errors; that is, the programmer has made an error in the interpretation or implementation of the specification. If the error has not been discovered and corrected during validation tests, it may eventually be discovered by the user. The observation of errors is a random process. Unlike physical failures, once they are discovered and corrected, design errors will not recur. However, an unknown number of new errors may be created in the process of correcting a known programming error.

Since data on design errors is scarce, there is no uniformly accepted evaluation model equivalent to MIL-HDBK-217E (military standard for computing the failure rate of specific types of integrated circuits). These types of software faults are generally termed permanent fault, being that the cause is an inadequacy in the design (or implementation) of the system. Transient faults are faults that are due to temporary environmental conditions that cannot be resolved by repair of the system. The main issue here is that even though software can be graded as highly reliable, transient faults can lead to system failure.

6.2.1 Fault-Tolerant Software Engineering

Software development processes and methods have been studied for decades. Despite that, we still do not have tools to guarantee that complicated software systems are fault-free. In fact, it may never happen that we will be able to guarantee error-free software. The reason is that the two basic ways of showing that software is correct, proof of program correctness and exhaustive testing, may never be practical for use with very complex software-based systems. Techniques for proving software correct (generally termed "formal methods") tend to work only for relatively small and simple synchronous systems, while testing methods, although increasingly more sophisticated, do not guarantee production of error-free code because exhaustive testing is not practical in almost all cases. Therefore, it is necessary to investigate techniques that permit software-based systems to operate reliably and safely even when (potential) faults are present.

General methods that have shown effectiveness in increasing the fault-tolerance of system software include: assertion testing (acceptance testing), algorithmic, recovery blocks, N-version programming. Assertion testing is a programmer provided, program specific, error detection mechanism that provides a check on the interim results of program execution. Relatively simple assertion tests would include testing boundary conditions (i.e., the interim result should not be any larger than "x"), and comparison/evaluation among two or more software variables (i.e., result x should be within $\pm$ 2 of result y). Depending upon the criticality of the potential failure, more extensive assertion checks can be developed but at the risk of increasing computation time, which may have undesirable side effects such as missing program scheduling deadlines or tripping watch-dog timers. In its strictest sense, assertion testing provides a means of fault detection. The "corrective" follow-up action is a graceful abort of the operation into some controlled, restartable state.

Algorithmic fault-tolerance is somewhat of an extension to assertion testing. For example, consider a block of data that is stored as an array. To help ensure that the data inserted into the table is correct, it can be checked by various assertions. Once in the table, algorithmic fault-tolerance methods can be applied to help ensure the consistency of the data. One such method is the generation of row and/or column checksums to detect and correct single bit errors and detect multiple bit errors.

Recovery blocks is a method of fault-tolerance that employs software redundancy and allows for detection and correction of an error. The process begins when the output of the first module is tested for acceptability. Generally the acceptability test is a simple assertion. If the test fails, it restores (or rolls-back) the state of the system before the first or primary module was executed. It then allows a second (backup) module to execute and applies the same acceptance test. There can be multiple backup modules. If none of the backup modules produce acceptable results, then the system fails.

N-version programming is another type of fault-tolerant redundancy scheme. It proposes parallel execution of N independently developed functionally equivalent versions with adjudication of their outputs by a voter. All of the N-versions receive the same data set on which to apply their computations. The outputs are evaluated by a voter and the correct output is chosen. Generally the correct output is chosen by simple majority, hence, an odd number of versions (i.e., 3) are developed and used. This method relies on multiple parallel computers which forward their results to a single, simpler voter machine. This method, while incurring the cost of multiple hardware configurations, allows for parallel execution of the alternate schemes, resulting in shorter latencies when a fault has been detected. This is the scheme used in many avionics systems; perhaps the best known is the space shuttle.

6.2.2 Software System Analysis

A common feature in the above mentioned fault tolerance schemes is some method of fault detection usually performed by applying some software test to system variables. In many cases, the reason for checking the specified variable stems from criticality issues determined during the system design. The development of reliability graphs which aid in the prediction of system reliability is closely linked to the values of the critical system variables. Fault trees, which is one particular type of reliability graph, is one of the most widely used methods for analyzing software systems. Fault trees provide a graphical and logical framework for analyzing the failure modes of systems (both hardware and software). Their use helps the analyst to assess the impact of software failures on an overall system, or to prove that certain failure modes cannot occur (or occur with negligible probability). Fault tree models provide a conceptually simple modeling framework that can be used to compare different design alternatives or architectures for fault tolerance.

A fault tree consists of the undesired top event (system or subsystem failure) linked to more basic events by logic gates. The top event is resolved into its constituents causes, connected by AND, OR, and M-out-of-N logic gates, which are further resolved until basic events are identified. The basic event represents basic causes for the failure, and represent the limit of resolution of the fault tree.

Analysis of the fault tree begins with an enumeration of the minimal set of component failures which cause system failure. This set is termed the minimal cut set. The minimal cut set contains a list of non-redundant elements that can cause the top event. Typically, for a complex system, many top failure modes can occur, and each will have a minimal cut set. Usually, the first step in analysis is to survey the minimal cut sets for any single point of failure. Single points of failure are identified by cut sets with a single element. In hardware-software systems for example, a single sensor can sometimes be identified as a single point of failure. Knowing this, adequate software fault detection (and correction) schemes can be developed to eliminate and minimize the probability of a specific failure mode.

Fault tree analysis emanated from the need to determine the reliability of hardware systems. The same method can be applied to software systems. For example, fault tree analysis can be applied to the recovery block and N-version programming methods discussed above to provide a qualitative design aid. Specifically, they can help the designer determine a good set of on-line reasonableness checks and off-line validation tests to cover a class of potential faults.

6.3 FAIL-SAFE ANALYSIS FOR DISTRIBUTED CONTROL SYSTEMS

Design of safe distributed control systems calls for special considerations of certain design aspects. Timing aspects, node error handling, and functional allocation between different nodes are important. For example, SAE J1939 has a number of different error detection mechanisms implemented that are used to increase the safety of the bus. CSMA/AMP bus access reduces the likelihood of a babbling idiot node fault; the use of a cyclic redundancy check reduces the likelihood of not detecting erroneous messages; and the differential signal encoding method used together with shielded twisted pair cable reduces the likelihood of electromagnetic interference causing bus errors.

The validation of a distributed control system requires the evaluation of aspects not present in a conventional control system. Current work in this area has suggested the need of new validation methods for distributed control systems (Ref. 10, 13). In order to get a safe distributed control system, it is especially important to detect and handle a number of fault types that are either completely unique for distributed systems or become much more important for distributed systems. Examples of such fault types are node faults, bus faults, timing faults, data consistency faults, initialization/restart faults, babbling idiot faults and configuration faults.

Questions to be considered for each type of defined fault are given below:

Node faults:

The operation of the control system is dependent on the correct operation of all nodes. Examples of questions to address by a fail-safe analysis are:

- Does a node in the system know the status (operational, idle, incorrect) of the other related nodes?
- What happens if a node is involuntarily disconnected; e.g., by a damaged cable?
- What action is taken when a node detects an internal error?

- What action is taken when a node detects an error in the surrounding system?
- Will a node continue to run its application software also when a large number of input signals are changed within a short time?
- Is there some mechanism to read back and compare important data between the nodes?

Bus faults:

- Bus faults are anything that will result in the loss of a message or the reception of an erroneous message. Examples of questions to address by a fail-safe analysis are:
- Are mechanisms in place to assure that an erroneous message is detected as it is sent from one node to another node?
- What action is taken when a node detects an erroneous message?
- What happens if the communication cannot be properly started?
- Can fault tolerance be achieved by use of double busses?
- Will a node continue to run its application software also when a large number of incorrect messages are sent on the bus?

Timing faults

Timing errors are perhaps most commonly addressed when discussing errors in distributed systems. Examples of questions to address by a fail-safe analysis are:

- How can you tell if the specified response time of the machinery is kept?
- Can the transfer time of a message be guaranteed?
- Are there guarantees that a node is not processing old data?
- Is the system robust for old data as odd events?
- How is a delayed message handled?
- How long is the start-up time on the distributed system?
- Can control algorithms be processed with adequate speed?

Data consistency faults:

These faults occur when cooperating nodes use data of different ages. Examples of questions to address by a fail-safe analysis are:

- Are there mechanisms to guarantee that a message will arrive at all destinations?
- Is there some mechanism to read back and compare important data between the nodes?

Initialization/restart faults:

These errors occur at the start up sequence of the control system. Examples of questions to address by a fail-safe analysis are:

- Is correct priority given to every node?
- Will all operation of the system not start before complete initialization?
- Which nodes may send out a request for restart?

"Babbling idiot" faults:

This term is used to describe when a node is constantly transmitting and occupying the bus.

- How is a node that is constantly transmitting and occupying the bus to be handled?

Configuration faults:

These faults are the result of user errors when connecting and configuring the nodes on the bus. Examples of questions to address by a fail-safe analysis are:

- Are all nodes of correct type?
- If parameterization is used, are all parameters correct; i.e., are all diagnostic parameters defined the same for all nodes and diagnostic devices?
- Is the used bit rate correct?
- Are all nodes using the correct communication protocol?

Currently there are no widely accepted formal methods for fail-safe analysis of a distributed control system, however, development work is underway. Indeed, the number of successful distributed control systems introduced in a variety of industries indicates a significant proprietary capability. Any future development work should include the addition of distributed control issues into formal analysis methods such as fault tree analysis (FTA) and failure mode and effects analysis (FMEA). Methods for both fail-safe analysis and testing will have to be considered.

7 COMPATIBILITY ISSUES

Compatibility is a multifaceted term that includes a number of interrelated issues that are essential to the definition of ECBS-brakes as a product. These issues address many of the differing opinions among stakeholders that need to be resolved before ECBS can gain widespread acceptance. The fleets' concerns related to resale value and obsolescence raises the question of backward compatibility. Will ECBS equipped tractors (trailers) be compatible with trailers (tractors) equipped with pneumatic/ABS brakes, and will newer more sophisticated versions of ECBS be compatible with older versions of ECBS?

Compatibility among brake manufacturers is also an important issue. There appears to be a consensus that compatibility among manufacturers should exist at the tractor/trailer level. That is, a tractor equipped with ECBS from manufacturer "A" should be compatible with a trailer equipped with ECBS from manufacturer "B". However, there is little agreement about compatibility and interoperability ability at the component level. Truck and trailer manufacturers wish to purchase braking components as a commodity from a number of suppliers, while brake manufacturers may wish to maintain a competitive advantage by marketing a proprietary product.

In this section we will attempt to frame many of the issues related to ECBS compatibility. It is not our intent to resolve these issues which are best resolved within an industry standards process at SAE and/or TMC.

7.1 ECBS CLASSIFICATIONS AND CONFIGURATIONS

In order to discuss the issues of compatibility, it is necessary to classify the wide variety of possible braking configurations. We have attempted to keep definitions within this section consistent with published definitions (Ref. 14, 15) wherever practical.

Definitions:

Pneumatic control circuit: A pneumatic control circuit is a pressure signal that is used to command a brake application. For standard pneumatic brakes this consists of the brake valve and the relay valve. System designs can have either 1 or 2 pneumatic control circuits. The nth pneumatic control circuit employed in a braking system is represented as Pn.

Electronic control circuit: An electronic control circuit is an electrical signal that is used to command a brake application. For ECBS brakes this includes the ECUs and a communications means between the ECUs. The nth electronic control circuit employed in a braking system is represented as En.

Working circuit: The working circuit supplied the energy for applying the brakes and includes the air pressure in the reservoir and the brake chamber. The nth working control circuit employed in a braking system is represented as Wn.

Tractor configurations:

Figure 2 illustrates the combinations of electrical and pneumatic circuits considered in this section. The control circuits are combined with two working circuits in multiple combinations.

Figure 2.a) is the conventional pneumatic/ABS system (0E-2P). If either the primary control circuit (P1) or the primary working circuit W2 fails, the vehicle is put into emergency brake by the backup circuits (P2, W2).

Figure 2.b) shows two possible electronic control systems with redundant pneumatic backup circuits (1E-2P).

(i) A single electronic control circuit (E1) is employed as a primary system for both working circuits (W1, W2). Two pneumatic control circuits (P1, P2) are equivalent to a standard pneumatic braking system and are employed as a backup system.

(ii) A single electronic control circuit (E1) is employed as a primary system together with the primary working circuit (W1). An independent pneumatic control circuit (P1) is employed

as a backup for working circuit #1 (W1). A second pneumatic control circuit (P2) and working circuit (W2) are employed as a complete second backup system.

Figure 2.c) shows four possible electronic control systems with single pneumatic backup circuits.

(i) A single electronic control circuit (E1) is employed as a primary system for both working circuits (W1, W2). A single pneumatic control circuit (P1) is employed as a backup system for both working circuits (W1, W2). The control of W1 with P1 is made possible using a decoupling valve.

(ii) E1 is employed as a primary system for both working circuits (W1, W2). P1 and W2 are combined as a backup system.

(iii) E1 is employed as a primary system for W1. P1 is employed as a backup system for W1 and W2.

(iv) E1 is employed as a primary system for W1. P1 and W2 are combined as a backup system.

Figure 2.d) shows four possible redundant electronic control systems. These systems are equivalent to Figure 2.c) with P1 replaced with E2.

(v) A single electronic control circuit (E1) is employed as a primary system for both working circuits (W1, W2). A second electronic control circuit (E2) is employed as a backup system for both working circuits (W1, W2).

(vi) E1 is employed as a primary system for both working circuits (W1, W2). E2 and W2 are combined as a backup system.

(vii) E1 is employed as a primary system for W1. E2 is employed as a backup system for W1 and W2.

(viii) E1 is employed as a primary system for W1. E2 and W2 are combined as a backup system.

Figure 3 illustrates the combinations of electrical and pneumatic circuits considered in this section for trailers. The control circuits are combined with one working circuit in multiple combinations. A minimum number of control and working circuits are presented. The additional control and working circuits will not affect the discussion of tractor/trailer compatibility.

Figure 3.a) is a conventional trailer service brake system (including ABS) (0E-1P).

Figure 3.b) is an electronic control system with a single pneumatic backup. This system requires two control lines (one electric one pneumatic) to the tractor.

Figure 2. Tractor brake configurations

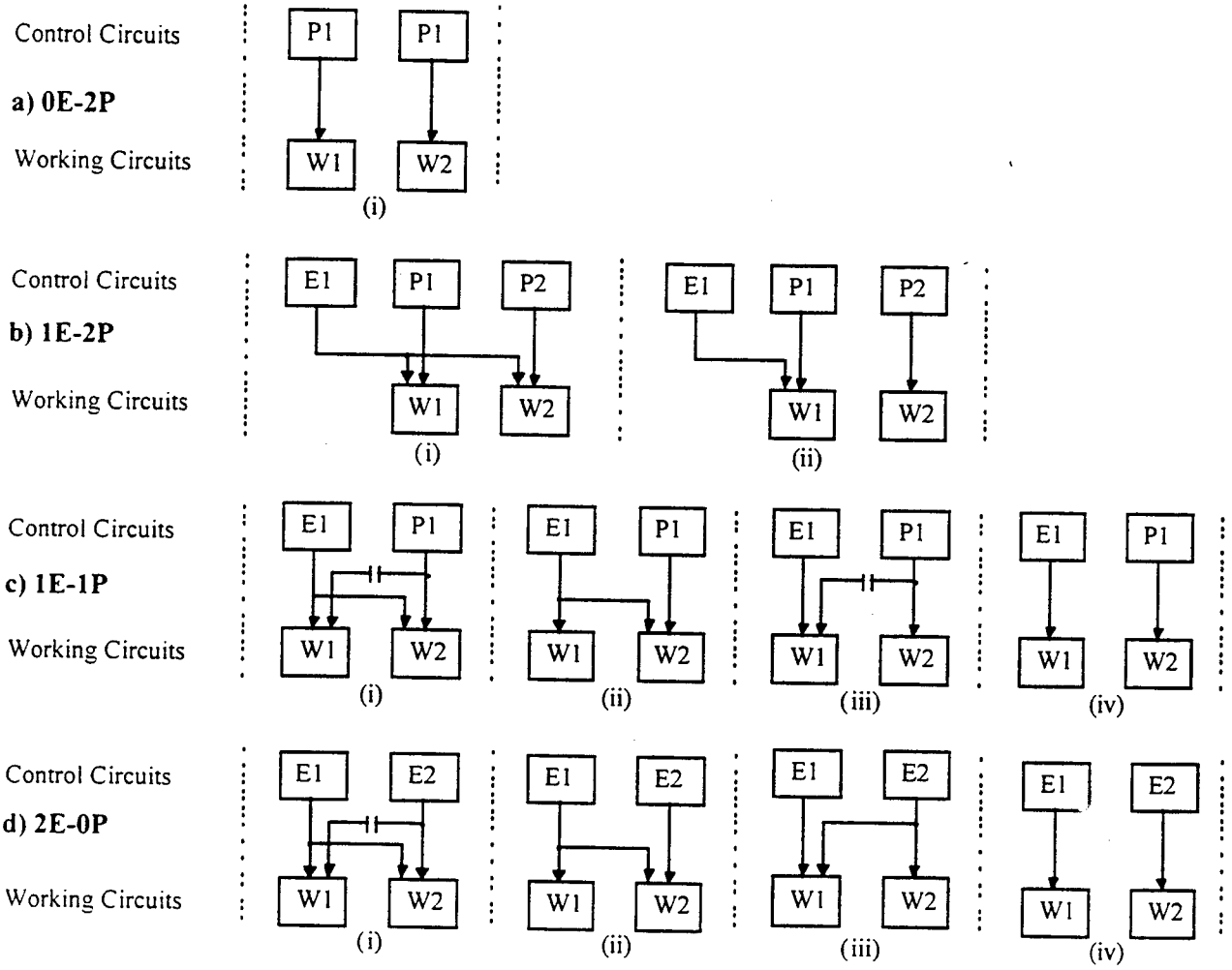
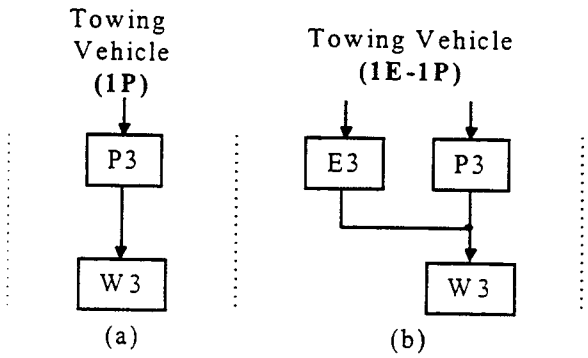


Figure 3: Trailer brake configurations



These simplified descriptions were selected as examples of dual circuit backup. For the tractor, a minimum of two control circuits are provided to control two working circuits. The backup is implemented in different ways. It should be pointed out that with the current system the backup is used to deploy emergency braking (fail silent mode). The cross coupled circuits, such as figure 2.d.(i), can provide for normal operator control after a failure occurs in the primary circuit (fail operational mode).

7.2 COMPATIBILITY WITH PNEUMATIC/ABS SYSTEMS

As mentioned above, it is desirable for ECBS to be compatible with standard pneumatic/ABS brakes. Standard pneumatic /ABS braking systems on tractors and trailers will be with us for some time. Expected life of this capital equipment is on the order of ten years. In addition, these systems will continue to be manufactured for the foreseeable future since ECBS is not likely to be mandated.

The level of compatibility desired is highly dependent on fleet operations. A private or LTL (less than truckload) carrier that has complete control over its tractors and trailers may not be concerned about compatibility. A TL (truckload) carrier that uses a large number of owner operators and tows a variety of trailers not under its direct control will be deeply interested in compatibility.

The compatibility of various pneumatic and electronic braking combinations is shown in Table 1. Five of the nine combinations shown above are sufficiently compatible to provide redundant control of both tractor and trailer brakes. Two of the combinations will provide for only non-redundant control of trailer brakes. Two combinations are not compatible (without additional equipment on either the tractor or the trailer).

The (0E-2P)-(1P) corresponds to a conventional tractor/trailer and provides redundant control of the tractor and trailer brakes.

Table 1 Tractor/Trailer Compatibility

		TRAILER		
		1P	**1E-1P**	**1E**
TRACTOR	**0E-2P**	**Yes[1]**	**Yes[1]**	**No**
	1E-1P	**Yes[2]**	**Yes[3]**	**Yes[2]**
	2E-0P	**No**	**Yes[1]**	**Yes[1]**

1) These four combinations provide the same level of redundant control as the standard pneumatic braking system.
2) These two combinations do not provide redundant control of the trailer brakes.
3) This combination provides redundant control of all braking functions plus a second control line between the tractor and trailer.

The (0E-2P)-(1E-1P) combination is functionally equivalent to the conventional tractor trailer combination. The (2E-0P)-(1E) is a totally electronic system providing the same level of redundancy as the conventional pneumatic system. The (2E-0P)-(1E-1P) combination is a totally electronic system providing equivalent redundancy as the conventional tractor/trailer combination. A potential weakness for these four combinations is that a single control line is used between the tractor and the trailer.

Only the (1E-1P) trailer is compatible with all three tractor systems. The (1E-1P) trailer combined with the (0E-2P) or (2E-1P) tractor provides the same level of redundancy as the standard pneumatic/ABS system. The (1E-1P)-(1E-1P) combination provides for redundant control of all brakes plus provides a second control line between the tractor and the trailer potentially improving system reliability.

The (1E-1P) tractor combined with the (1P) or (1E) trailer will function but will not provide redundant control of the trailer brakes. Redundant control can be provided for these combinations if additional capabilities are added to the tractor or trailer. (See discussion below.) The (0E-2p)-(1E) and (2E-0P)-(1P) combinations are not compatible unless additional capabilities are added to the tractor or trailer.

It is claimed (Ref. 14) that "the fully electric brake by wire system (2E) does not have any functional advantages nor are there any cost savings if you take into consideration the additional battery." This logic would lead to the selection of 1E-1P as the standard for both tractors and trailers. The added reliability of a second control link between the tractor/trailer is an additional plus for this combination. Compatibility problems are also less of a concern for the (1E-1P) approach.

Other opinions in the industry see the 2E-0P combination as the low cost final solution for ECBS. To get to this final solution, intermediate steps need to be taken to assure compatibility. These intermediate steps include adding additional equipment to the tractor or trailer for those customers who are interested in compatibility during the transitional period.

Compatibility with 0E-1P trailers with the 2E-0P tractor can be obtained by adding an E to P converter. This would involve adding an additional pressure control loop on the tractor to create the pneumatic control circuit for the trailer. Adding a P to E converter on the (1E) trailer would allow compatibility with 0E-2P tractors. This involves adding to the trailer a pressure sensor and appropriate electronics (analog to digital converter) to generate a digital signal which can be used as a reference for the electronic control loops in the trailer.

For each solution put forward, a number of additional compatibility issues should be considered. The most obvious is the interface between the tractor and the trailer. For full compatibility, the interface must include:

1. a pneumatic supply line

2. a pneumatic control line

3. an ABS/ECBS power connection

4. a communications connection (employing a well defined communications protocol)

Techniques must also be developed for automatically identifying the trailer type that is connected. The compatibility of the tractor /trailer (or lack thereof) could be presented to the driver as part of the user interface. It is of primary importance that the vehicle brakes are not released if the systems are incompatible.

Synchronization of tractor trailer brakes is also important. A brake system of a tractor/trailer combination is considered well synchronized if any differences between tractor and trailer delay times and crack pressures are kept to a minimum (Ref. 21). The potential for significant variation in brake synchronization ECBS equipped tractors and pneumatic/ABS equipped trailers is a problem that must be addressed for tractor trailer compatibility.

How the backup systems are employed when the primary control circuit fails must also be considered. If the tractor's (trailer) primary circuit fails, what action will be taken? How will the trailer (tractor) know when to switch to a backup circuit? Will emergency brakes be applied or will the operator maintain control of the backup system? For full compatibility, standards will need to be generated that prescribe how this switch-over occurs for all combinations of tractors and trailers.

It is not clear at this time whether the pneumatic backup system associated with the (1E-1P) systems will include independent ABS capabilities. It can be argued that ABS functionality is not needed for a backup system which is intended to be used for short periods. It can also be argued that failure could take place during a braking maneuver when ABS is needed.

7.3 COMPATIBILITY AMONG BRAKE MANUFACTURERS

Compatibility among manufacturers is a complicated issue. Given the wide variety of ECBS combinations that may exist, the varying and potentially conflicting stakeholder opinions, sorting out all the variables will be a daunting task. Decisions made in this area will most certainly effect decisions related to ECBS configurations discussed in the last section. It is not the intent of this report to resolve these compatibility issues. These issues are best resolved through industry groups such as TMC and SAE.

7.3.1 Tractor/Trailer Compatibility

There appears to be a consensus among stakeholders (fleets, brake manufacturers, truck manufacturers and government) that ECBS should be compatible at the tractor/trailer level. A tractor equipped with company A's ECBS should be compatible with a trailer equipped with company B's ECBS. This demand places a number of constraints on the design of a system. A common communications protocol must be used for all compatible systems. The system must be defined sufficiently to assure true interoperability. In addition, it may be necessary to standardize some of the functional aspects of the systems. This can also be part of the communications protocol interoperability guidelines.

If absolute compatibility is desired, then this demand would likely limit the number of features included in an ECBS-braking system. Specifying a minimum level of compatibility, however, would allow manufacturers to add product distinguishing features that would only be fully used if

their system is employed on both tractor and trailer. This is important with regard to innovation and the development of ever improving braking systems. The issue here is backward compatibility; that is, a minimum standard for tractor/trailer compatibility could also be applied to different generations of ECBS from the same manufacturer.

Communications protocol and compatibility (interoperability)

The level of interoperability for the communications protocol required for true compatibility is "plug and play." This is the highest level of interoperability for communications. Plug and play simply means that when a component (a tractor or trailer, in this case) is exchanged, the system will function normally with no adjustments.

To achieve plug and play compatibility, all aspects of the communications protocol must be defined. A key issue is the connector. A number of potential standard connectors have been put forward, but no U.S. standard yet exists. Many of the remaining issues to be considered are specified or will be specified in SAE J1939. One of the key issues is determining the number of messages to be sent from the trailer to the tractor. The number of ECUs used on a trailer can vary for a number of reasons including varying number of axles and variations in design philosophies.

Although work is underway, the SAE J1939 standards has not completely addressed these issues. The committee intends to adopt a European solution to tractor/trailer compatibility that uses a bridge between the tractor and the trailer to filter the messages and provide a uniform set of information independent of internal configurations.

The current set of messages provided by SAE J1939 for ECBS will likely need to be updated and new messages may need to be created. Currently SAE J1939 defines two messages for brakes. These messages are discussed below.

SAE J1939 Message 3.3.4 -Electronic Brake Controller #1

This message contains 8 bytes of which 3 are defined. Byte #1 is used for ABS and ASR (traction control) status information. Byte # 2 is a digital representation of the brake pedal position. Byte #3 is used to represent control switch positions for ABS and ASR. Bytes #4 -8 are undefined. A repetition rate of 100 ms is prescribed and a priority of 6 is defined: (This message will not be transmitted until all pending messages of priority 5 and lower are transmitted).

Transmission repetition rate:	100 ms
Data length:	8 bytes
Data page:	0
PDU format:	240 (group extension addressing)
PDU specific:	1
Default priority:	6
Parameter group number:	61,441(00F00116)

Byte:	1	Status_EBC1	Bit:	8-7	Not defined
				6,5	ABS active
				4,m3	ASR brake control active
				2,1	ASR engine control active

2	Brake pedal position			Numeric
3	Status_EBC1	Bit:	8-7	Not defined
			6,5	ABS active
			4,m3	ASR brake control active
			2,1	ASR engine control active

SAE J1939 Message 3.3.40 - Brakes

This message contains 8 bytes of which 4 are defined. This message contains brake status information. Byte #1 is a digital representation of the brake application pressure. Byte # 2 is a digital representation of the brake primary pressure (supply side pressure). Byte #3 is a digital representation of the brake secondary pressure (service side pressure). Byte #4 is used for encoding brake status. A repetition rate of 1 sec. is prescribed and a priority of 6 is defined: (This message will not be transmitted until all pending messages of priority 5 and lower are transmitted).

Transmission repetition rate:	1 sec
Data length:	8 bytes
Data page:	0
PDU format:	254
PDU specific:	250
Default priority:	6
Parameter group number:	65,274(00FEFA16)

Byte:	1	Brake application pressure (measured at brake chamber)			
	2	Brake primary pressure (supply side pressure)			
	3	Brake secondary pressure (service side pressure)			
	4	Brake status	Bit:	8-3	Not defined
				2,1	Parking brake actuator
	5-8	Unused			

It is not clear whether these messages are sufficiently defined. Questions to be answered are:

- Is the message priority appropriate?
- Should additional diagnostic information be added to one or both of the above messages?

Will other sensor information be added to the brake ECUs and the associated messages, or will this sensor information be obtained through the network?

7.3.2 Component Level Compatibility

Going beyond tractor/trailer compatibility to component level compatibility is a desirable feature from the fleets' point of view. This will allow the fleets to obtain component parts from several manufacturers reducing the cost through competition. The manufacturers, on the other hand, wish to differentiate their products based on competitive design features. The degree of component level compatibility will be determined by the marketplace and through stakeholder interaction within industry organizations such as SAE and TMC.

Component level compatibility calls for standardizing all aspects of the ECBS design. This will involve several standardization efforts working together with SAE and TMC. The goal of these standardization efforts is to sufficiently design the ECBS systems so that each component can be defined in terms of functionality, mechanical interfaces, electrical interfaces, and pneumatic connections.

A decision will need to be made with regard to the number of ECUs employed on both the tractor and the trailer. Will an ECU service an axle or a wheel? Sensor and actuator connections will need to be specified including connector type, signal definition, and electrical properties of the signal. Common mounting strategies for each component will need to be standardized. Finally, the pressure control loops will also need to be standardized. This will involve specifying the accuracy and timing of the control system.

8 SENSORS FOR DIAGNOSTICS AND IMPROVED BRAKING PERFORMANCE

Initially ECBS will incorporate a limited sensor package. Sensors for monitoring supply tank air pressure, brake chamber air pressure, and an ABS wheel sensor can provide sufficient capabilities for fielding ECBS. Additional information regarding the status of the communications bus will also be available to the diagnostic system. Even this limited set of information can be used to provide a significant diagnostic capability. Diagnostic capabilities and brake functionality can be considerably enhanced by introducing additional sensors.

8.1 BRAKE DIAGNOSTIC SENSORS

Brake system monitoring can be divided into brake status monitoring and brake performance monitoring. As defined in a recent FHWA study of onboard diagnostic equipment (Ref. 16), brake status monitoring is intended to "monitor key variables that correlate to impending system failures." Here the definition of brake status is modified as: "*static measurements (vehicle not moving) that can correlate to impending system failure.*"

Brake performance monitoring is defined as: *dynamic measurements (vehicle moving) that can correlate to impending system failure or indicate serious system performance degradation.* Performance monitoring can result in an immediate notification to the driver of a problem or a storage of information about selected brake applications. This historical information is stored on the vehicle for later access by authorized personnel. The system can be designed to store sensor information for the last several brake applications and/or for braking applications that involve extreme conditions. For example, a set of historical braking information may include all sensor reading for the last 5 brake applications and for braking applications when ABS was activated and when maximums were observed for brake shoe temperature, brake chamber pressure, and brake torque.

ECBS brake system status and performance can be determined by monitoring brake adjustment parameters (push rod stroke or brake shoe travel), brake lining wear, brake system air leaks (brake chamber pressure and/or compressor duty cycle), brake torque, brake shoe temperatures and communication bus status. The relationship to brake function for these parameters is discussed below:

- Brake adjustment / push rod stroke (brake status)

  The current method for checking brake adjustment utilizes a measurement of push rod stroke during a static brake application. While the inspector is underneath the truck, the driver is instructed to apply the brakes. The inspector notes the push rod travel and compares this with a maximum allowable value. A sensor to measure push rod stroke or alternatively brake pad travel would eliminate the need for manual inspection of brake adjustment.

- Brake shoe thickness (brake status)

  When possible, brake shoe thickness is measured during roadside inspection. This inspection is done visibly if an inspection dust cover or sight hole is provided. If no opening is provided to inspect the shoe, the measurement cannot be made without removing the wheel assembly. In these cases, brake linings are not inspected at the roadside. A brake lining sensor would eliminate the need for manual inspection of brake linings.

- Brake system air leaks (brake status and brake performance)

  Brake system air leaks are a critical part of roadside inspections. Roadside inspectors check for air leaks simply by observing the air reservoir gauge and by simply listening to them. The procedure is to have the driver run the engine at idle and then apply and hold the service brake. The inspector observes the air reservoir gauge on the dash until it drops to 80 psi. At that point, the compressor should activate and the air pressure should remain the same or increase. A drop in pressure indicates a serious leak in the air system.

  An onboard method for detecting air leaks could include adding diagnostic software to interpret the reservoir air pressure signal in the same manner as the inspector. This would involve no additional sensors. An alternate method would be to correlate air compressor activity with leaks. To distinguish leaks from frequent or heavy brake activity, it would be necessary to correlate brake activity (as observed on the communications bus) with compressor activity.

- Brake torque sensor (brake performance)

  Brake torque sensors can provide direct evidence of reduced braking efficiency. It does not, however, identify the root cause of the problem. If the brake torque sensor is used as part of the active control loop, an inability to supply the commanded brake torque would result. If the torque sensor is not used as part of the active control loop, the resulting torque could be compared with the expected torque given the pressure in the brake chamber. The driver could be warned about a serious reduction in braking torque by using a lamp or other user interface. In addition, the time and sensor information related to the low torque event could be stored for later retrieval by inspectors or maintenance technicians.

- Brake temperature sensor (brake performance)

  Brake temperature is currently not actively monitored. Maintenance technicians do, however, look for signs of high temperature such as discoloration of metal parts. By measuring the temperature of the brake shoe, the driver could be warned by using a lamp or other user interface. This information could help a driver avoid the situation of brake fade due to

excessive brake shoe temperature. In addition, the time and sensor information related to the high temperature event could be stored for later retrieval by inspectors or maintenance technicians.

- Communication bus status (brake status and brake performance)

  Communications bus failure constitutes a serious brake failure. As with the sensor related problems, a failure of the communications bus that lasts for more than a specified period of time could be communicated to the driver and stored as a time-stamped event for later retrieval by inspectors or maintenance technicians.

8.2 DIAGNOSTIC TOOLS

For diagnostic capabilities to be most effective, properly designed diagnostic tools must be available. The design of the diagnostic tools is an important part of the communication protocol standard. Diagnostic tool design raises issues related to standardization of diagnostic information within a braking system and security measures. A diagnostic tool includes a means of accessing the diagnostic information (a query method), a means to interpret diagnostic information, and a means for displaying the information to the operator (driver, technician or inspector).

Onboard diagnostic displays currently being considered include red and yellow light indicators to the driver. The red light indicates a serious brake failure while the yellow light indicates a minor brake defect. ECE regulation R-13 has specified a set of light indicators for tractor trailer combinations. Four lights are used: a red-yellow light pair is used for indicating tractor faults, and a second red-yellow light pair for indicating trailer faults. It may also be useful to provide the driver with a means of accessing fault codes which can be communicated to maintenance personnel or dispatchers.

Maintenance personnel will require a much more sophisticated diagnostic tool. Some sort of alphanumeric and/or graphical display will likely be necessary. The system, depending on its complexity, can be a hand-held device, a laptop or desktop computer. In either case, the diagnostic device should be able to access all brake status and stored brake performance information. The diagnostic tool should be designed for intuitive operation reducing the training required for the technician and reducing the potential for misinterpreting information.

Roadside inspection will require a diagnostic tool similar to that for maintenance personnel. The main difference will be security measures that will be built into either the onboard network or the diagnostic tool. The inspector will only have access to information required by the inspection protocol. The network link to the inspector will also need to be considered. A wireless link will ensure that connecting the diagnostic system does not introduce electrical faults into the system and may provide a means for gathering inspection information without stopping the vehicle.

8.3 SENSORS FOR ENHANCED BRAKING CAPABILITIES

ECBS stopping capabilities may be enhanced through the addition of appropriate sensors. The sensor information would be used to modify the control of brake chamber pressure for each wheel in an attempt to provide shorter and more controlled braking maneuvers. The possibility of adding

sensors for the purpose of advanced control of braking and handling is given below. Braking strategies will be discussed at a very general level and no attempt will be made to determine the merit of any specific strategy.

It is important to point out that most of the braking strategies considered are a compromise between total stopping distance and vehicle control. (Stopping distance usually must be lengthened to obtain more control.) In addition, automated braking strategies remove decision making from the driver who can adjust his braking strategy based on the situation. The appropriateness of any specific braking strategy should be carefully analyzed for effectiveness in avoiding and reducing the severity of crashes under a variety of driving conditions.

The addition of multiple sensors to a braking system could also negatively impact the system reliability. The consequences of sensor failure should be carefully scrutinized as part of a formal fail-safe analysis.

Sensors for advanced braking strategies:

- Torque sensor:

  A direct measurement of braking torque would provide the most direct measurement of braking effort for each wheel. With the application of a brake torque sensor, a braking command could be interpreted as a request for a specific braking torque rather than a brake pressure. Within the accuracy of the sensors, the braking for all wheels can be precisely balanced.

- Axle load sensor:

  A direct measurement of axle load would provide a means for adjusting the brake pressure (or brake torque if used in conjunction with a torque sensor) for each axle. This could, in principle, reduce stopping distances (Ref. 14, 15). Brake pressures are controlled for equal friction loading. This results in reducing the onset of ABS as long as possible.

- Coupling force sensor:

  A coupling force sensor can be used to minimize the forces between the tractor trailer during braking.

9 REGULATORY ISSUES

Within the current regulations (FMVSS No. 121) (Ref. 17), ECBS are not allowed. In this section we will explore a number of issues related to the modification or adoption of regulations that would allow various forms of ECBS. Regulations that consider ECBS as an allowed option are considered. No consideration is given to the possibility of mandating ECBS.

Efforts are currently underway to establish performance criteria for pneumatic braking systems (Ref. 18, 19). These efforts are focused on the in-use performance of braking systems. Issues being considered are braking component variations that can degrade braking performance, and inspection and test procedures that can be used to identify component related problems.

These issues, for the most part, are outside the scope of this effort. The discussion here will be confined to issues related to ECBS. However, issues related to overall brake and overall electronic systems' performance will be discussed at a general level.

9.1 REGULATORY ISSUES AND STAKEHOLDER COMMENTS

ECBS specific regulatory issues to be considered are listed below together with a summary of stakeholder comments.

A list of the questions asked to the identified stakeholders and a summary of the responses to each question are given below:

- What variations of ECBS should be allowed within the regulations?

  A consensus opinion among the stakeholders is in favor of allowing all redundant combinations of ECBS.

- Should FMVSS No. 121 be modified to allow ECBS or should a new performance based regulation be established for all braking systems?

  Most of the interviewed stakeholders were in favor of new performance based regulations. The industry as a whole appears to view prescriptive regulations such as FMVSS No. 121 as an impediment to innovation. In addition, a number of stakeholders observed that it is difficult to prescribe safety into the design of a complex system involving electronics, software, and asynchronous communications.

- What specific changes should be made to FMVSS No. 121 to allow ECBS?

  A document suggesting possible changes to FMVSS No. 121 for the addition of ECBS has been produced by the SAE Truck and Bus Task Force-Future Brake Systems Forum. This document is reproduced in the next subsection as an example of how FMVSS No. 121 can be modified to include ECBS. The document represents a recommendation for minimal changes to the regulations. The document does not address the issue of fail-safe performance (electronics, software, and communications safety) in any depth.

- Should stopping capabilities requirements for ECBS be different than for standard braking systems?

  There appears to be little agreement over defining stopping capabilities within a regulation. The collected opinions covered a wide range of opinions and included the following divergent views: "The stopping capabilities for ECBS should not be different than those specified in FMVSS No. 121"; and "The brakes should be able to safely stop the vehicle under all driving conditions."

- Should regulations address compatibility among different brake manufacturers? Should regulations address compatibility with older pneumatic/ABS? Should SAE J1939 be mandated as the inter-vehicle communications standard for ECBS?

Most interviewed stakeholders agreed that these three issues are best resolved at the voluntary standards level. Efforts within SAE and TMC are currently addressing these issues.

- At what level should system safety/ fault tolerance (electronic, communication, and software safety) be addressed in the regulation?

  Here also, there is little agreement among the stakeholders. Comments ranged from regulations should hold manufacturers responsible for the safety, reliability, durability, and maintainability of the systems throughout the product life cycle to regulations should not address these issues.

9.2 POSSIBLE CHANGES FMVSS No. 121

A report has been produced by the Heavy Duty Brake Manufacturers Association that suggested changes for FMVSS No. 121 to allow ECBS (Appendix A1). The document addresses a number of definitions and attempts to parallel many of the pneumatic requirements with "equivalent" electronic requirements. For example, batteries used for ECBS are compared to air reservoirs. The document briefly addresses the issues of fault detection and indicator lamps for the driver. The issues of tractor trailer compatibility are also addressed. The important issue of fail-safe performance is not addressed in any depth.

If the regulation is to consider fail-safe issues, specifications for operation and testing of each ECBS node (ECU and associated sensors) will need to be added. The specifications should assure that the node will operate or fail-safe under all operating conditions. Each node has the potential to fail. The questions are how likely is the node to fail and how will these potential failures manifest themselves.

For example, consider the pressure sensor used in brake sensor control loop. If the pressure sensor fails, will it fail in a high state (maximum pressure reading), a low state (minimum pressure reading) or in an unknown state (serious change in calibration)? Will redundant sensors be used to assure that a single sensor failure can be identified? What action will be taken if a failure occurs? Will exception messages be defined to inform the other nodes and the driver of the error and the severity of the error?

In addition, network failures will need to be considered. The addition of network failures is complicated since non-ECBS nodes on the network can be the cause of communications failure. Some have suggested that a separated ECBS subnet be employed to avoid this problem. Also network failures can effect one or all of the braking nodes. This can lead to a multitude of situations where some nodes are operating normally while others have lost communications.

9.3 AAR SPECIFICATIONS FOR ELECTRONIC BRAKING SYSTEM FOR FREIGHT TRAINS

The work done by the American Association of Railroads (AAR) in the area of electronic brakes for freight trains can provide some guidance for changing FMVSS No. 121. The AAR has developed a design specific specification for ECBS. The specification, based on over five years of design and testing, was adopted in May 1997. The four documents that make up the specification deal with many of the important issues related to safety critical systems.

The AAR specifications include a number of important issues related to fail-safe operation. Although the failure modes applicable to rail applications are not necessarily applicable to trucks, the AAR specification can still provide some guidance.

The AAR specification is currently comprised of four documents: S4200, S4210, S4220, S4230. These documents are reproduced in Appendix A-2, A-3, A-4, A-5. A brief review of these documents is given below.

S4200 PERFORMANCE REQUIREMENT FOR TESTING ELECTRICALLY CONTROLLED PNEUMATIC CABLE-BASED (ECP) FREIGHT BRAKE SYSTEMS

The overall objectives of this specification are;

1. Assure that the performance of electrically controlled pneumatic (ECP) freight brake systems is uniform and consistent among equipment from different manufacturers.

2. Assure that cars equipped with AAR approved ECP brake systems from different manufacturers can be operated together in any electrically braked train.

3. Assure that AAR approved electric brake systems meet a high standard level of safety and reliability.

S4210 PERFORMANCE SPECIFICATION FOR ECP BRAKE SYSTEM CABLE, CONNECTORS AND JUNCTION BOXES

Objective:

To establish the qualification test procedure for an electric brake trainline connector, cable and end-of-car junction box. The qualification test procedure is intended to verify that the designed components have high reliability, will withstand harsh environmental conditions, and have a minimum of an 8-year operating life.

This standard applies to ECP brake system power and signal cable intended for use on interchange freight cars and locomotives equipped with AAR-approved ECP brake systems.

S4220 PERFORMANCE SPECIFICATION FOR ECP BRAKE DC POWER SUPPLY

Objective:

The purpose of the ECP power supply is to provide the battery charging supply from the locomotive(s) in the consist (train) to each car, through the hardwire trainline, sharing the same conductors with the communication signals (power line overlay mode). It is therefore essential that the quality of the electrical power supplied to the line be sufficiently well controlled so as not to interfere with the communications.

S4230 INTRA-TRAIN COMMUNICATION SPECIFICATION

This specification is to define the requirements for an intra-train communications system for freight equipment in revenue interchange service. The specification is intended to facilitate interoperability between freight cars and locomotives, without limiting the proprietary design approaches used by individual suppliers.

9.4 DESIGN NEUTRAL PERFORMANCE BASED REGULATION

Within a performance based regulation, the requirements for ECBS stopping capabilities can likely remain as stated in FMVSS No. 121. The addition of stopping tests that demonstrate the added benefit of ECBS control can be considered but are not essential. A more complex aspect of a performance based regulation is specifying the system safety and reliability (fail-safe operation).

ECBS is a double-edged sword as it pertains to the safety and reliability of braking systems. As discussed in previous sections, advanced electronic control techniques may provide for improved braking performance and improved vehicle control in a variety of situations. In addition, advanced diagnostic features of ECBS, when equipped with the proper sensor input, can provide a continuous assessment of the vehicle braking capabilities. Diagnostic capabilities can also provide for a more efficient and effective roadside inspection.

On the other side, complex systems involving electronics, software and communications are subject to unexpected and unpredictable failures. This potential for unexpected failures is greatly reduced through the application of appropriate design processes and failure analysis techniques.

Specifying performance standards within a regulation for fail-safe operation is a difficult task. To investigate this approach it appears wise to consider standards and methods from other industries with more experience in these areas. The FAA has a long history of successfully developing and applying performance based regulations for complex electronic systems. (A review of applicable FAA regulations is given in Appendix A-6.)

9.4.1 FAA Regulatory Model

As an exercise, an attempt to adapt the FAA regulatory language to ECBS is given below. This information is presented not as a proposed regulation but as a starting point for discussion. In this exercise it should be remembered that the fail-safe requirements for aircraft are considerably more stringent than what is needed for a ground vehicle. Aircraft systems must be designed to "fail operational" standards. That is, the aircraft systems must continue to function (remain in the air) when a fault or series of faults occur. Ground vehicles can and are designed for "fail silent" operation. That is, when a fault is detected, the vehicle is stopped. Fail silent operation is easier to achieve and results in lower development and system component costs.

The following is one possible adaptation of language used in FAA regulations applied to ECBS. Changes to the FAA language have been made to include language for fail silent performance to the existing language for fail operational performance.

Modified FAA Regulations

(a) The equipment, systems, and installations of ECBS equipment must be designed so that they:

(1) perform their functions under any foreseeable operating conditions, or

(2) safely stop the vehicle when a serious fault occurs.

(b) The ECBS and associated components, considered separately and in relation to other electronic systems, must be designed so that:

(1) the occurrence of any failure condition which would prevent the continued safe driving or stopping of the vehicle is extremely unlikely or is detectable by the system;

(2) the occurrence of any other failure (with non ECBS electronic equipment) would either not reduce the effectiveness of the system or be detectable by the system.

(c) Warning information must be provided to alert the driver to unsafe operating conditions and enable him to take appropriate action. System controls and associated warning systems means must be designed to minimize driver errors which may create additional hazards.

(d) Compliance with the requirements of paragraph (b) of this section must be shown by analysis (FEMA, FMECA, Fault Tree Analysis, etc.) and where necessary, by appropriate tests. The analysis must consider:

(1) possible modes of failure, including malfunctions and damage from external sources;

(2) the probability of multiple failures and undetected failures (this could be changed to any single failure);

(3) the resulting effects on the vehicle and driver, considering the possible vehicle operating conditions; and

(4) the driver warning cues, corrective action required, and the capability of detecting faults.

The very general language used above and in the FAA regulations signifies the fact that it is difficult to prescribe safety and reliability for complex systems. Safety for such systems can be best achieved through the application of appropriate design processes and analysis and testing procedures.

Regulatory Compliance

Within a generally worded performance-based regulation one must consider how regulatory compliance is achieved. The FAA takes a very active role working with aircraft manufacturers and carriers to assure that the systems are adequately analyzed and tested. This costly and time consuming approach is probably not applicable to the trucking industry. Some level of self-compliance seems more appropriate.

The ECE is currently considering a form of self compliance that may be applicable. The concept is to develop an ISO 9000 type procedure for self compliance (ECE regulations are discussed in

Appendix A-7). The procedure will clearly define all aspects of the compliance process including analysis, testing, and all associated documentation.

In addition to the general language about safety and reliability, a number of more specific minimum standards could be added. The manufacturers would be free to design and implement systems that represent an improvement over the minimum standards. In addition, incentives could be provided to encourage fleets and manufacturers to add desirable features to the system. Examples of minimum standards and incentive-based features are given below:

1. Compatibility

In any regulation, specific language will be needed to assure that the potential incompatibility of tractors and trailers does not pose a safety risk. As discussed in the section on tractor/trailer compatibility, there are a number of options for obtaining compatibility. SAE and TMC are the appropriate forums for developing compatibility specifications.

2. Diagnostic capabilities

As discussed in a previous section, the most basic ECBS systems will include sensors for pressure regulation and wheel sensor for ABS operation. The system will also have knowledge of the communication status. Based on this information, a minimum level of diagnostic information can be specified within a regulation together with storage and display requirements.

Additional sensors can also be considered. These sensors can be selected to provide a more complete real-time onboard diagnostic information or to provide a more complete set of information for roadside inspection. The addition of these sensors can be a regulatory requirement or can be part of an incentive package. The major benefit to the fleet for this package would be reduced roadside inspection burden.

3. Minimum safety analysis and testing

In general, effective safety assurance processes are being applied within the industry. Major manufacturers of ECBS likely employ sophisticated safety analysis procedures to assure the safety and reliability of their products. As discussed in previous sections, a variety of techniques can be used to obtain the desired outcome. In addition, standards exist for FEMA analysis within SAE (Ref. 20).

A performance regulation may wish to address this area to assure that competitive pressures do not unduly influence manufacturers to cut corners. This may be of particular concern for small companies that wish to produce third part replacements for braking systems. If this were the case, several steps could be taken to assure that an appropriate safety analysis is carried out. Regulations could specify the SAE FEMA standard as a minimum requirement that could be replaced by an equivalent or superior process. The SAE FEMA standard may need to be updated to better include software safety and reliability.

In addition, regulations could provide manufacturers with analysis requirements such as a list of potential hazards (i.e., uncommanded brake application, loss of brake pressure) to be considered in the safety analysis process.

9.5 CLOSING REMARKS

ECBS, as the first of several safety critical electronic systems to be installed on heavy trucks, represents an opportunity to develop a technology independent framework for safety assurance. A design-neutral systems approach to safety assurance can provide a high level of confidence within a regulatory model that will encourage advancement of technology and safety assurance methodologies.

To accomplish this, a substantial level of communication and cooperation among all stakeholders will be needed. Efforts currently underway within SAE, TMC, and at ITS America offer the best settings for accomplishing these goals. It is recommended that NHTSA and FHWA play an active role in these efforts in order to facilitate the cooperation of the industry stakeholders and to better understand the needs of this rapidly evolving industry.

10 9 RECOMMENDATION FOR FURTHER STUDY

10.1 TRACK TESTS

The next step in the evaluation of ECBS is to carry out a series of track tests that will quantify a number of performance and compatibility features. This effort will require a significant level of cooperation between an independent test organization (ITO), and industry partners (primarily the brake manufacturers and the truck manufacturers). The industry partners' primary responsibility will be to provide the tractors and trailers equipped with ECBS. The ITO's primary responsibility will be to impartially carry out the tests and data analysis. The ITO and industry partners will work together with other industry stakeholders to define a detailed test protocol and associated data collection systems.

The test protocol can address a number of ECBS issues including stopping distance, vehicle control during stopping maneuvers, and tractor/trailer compatibility. The test protocol should be carefully crafted to highlight the benefits of ECBS. It is also important that the detailed test protocol be acceptable to all industry stakeholders. An industry forum, such as the SAE Future Brake System Forum, is an appropriate venue for presenting the test protocol for industry comments. The tests should measure stopping distance and other important parameters associated with vehicle control and tractor/trailer compatibility. This will include combinations of tests on straight and curved tracks each with normal friction, reduced friction and split friction surfaces (half the wheels on a normal friction surface and half on a reduced friction surface).

Tractors and trailers equipped with a (1E-1P) ECBS configuration are the best choice for these tests. The (1E-1P) systems provide compatibility with conventional tractors and trailers. For this reason the (1E-1P) system is expected to be the standard for some time (Ref. 21).

The data collection system must acquire the information needed to quantify the capabilities of the various combinations of braking systems. Stopping distance can be measured simply with markings on the track or by using an optical range finder. Vehicle control can be best quantified by employing accelerometers and yaw rate sensors in key locations on the tractor and trailer. Tractor/trailer compatibility can be measured by monitoring the pressure for each wheel in order to determine the synchronization of brake application (Ref. 21). Measuring the coupling force

between the tractor and the trailer will also provide an indication for tractor/trailer compatibility.

The stopping capabilities of ECBS systems in various tractor trailer configurations can be tested and compared to stopping performance for a standard pneumatic/ABS brake system. Potential configurations to be tested include:

- Conventional pneumatic /ABS system
- ECBS tractor and conventional trailer
- ECBS tractor and trailer

By including these three configurations, the benefits of the full ECBS and tractor only ECBS can be directly compared to the conventional braking system.

10.2 TECHNICAL REVIEW OF CRITICAL SOFTWARE DEVELOPMENT PROCESSES

A number of recent advancements have been made in software risk management under sponsorship of ARPA at the Carnegie Mellon Software Engineering Institute. As with earlier work in electronic risk management, such as FMEA, these processes are becoming a requirement for military systems. They are also beginning to flow from the military to the commercial sector. Examples of formal processes that apply to ECBS and other onboard safety systems are:

The Capability and Maturity Model (CMM)

The Capability Maturity Model for software describes the principles and practices underlying software process maturity in terms of an evolutionary path from an ad hoc chaotic process to a mature disciplined process. The defined maturity levels are:

1. initial
2. repeatable
3. defined
4. managed
5. optimized

The effectiveness and reliability of the software developed is believed to increase as the software development process moves up the five levels.

Rate Monotonic Analysis (RMA) for Real Time Systems

RMA is a collection of quantitative methods that enable real time system developers to understand, analyze, and predict the timing behaviors of real time systems. The proper application of this methodology can lead to a better understanding of the risks involved in a safety critical software system.

Team Risk Management (TRM)

Team Risk Management defines the organizational structure and operational activities for managing risks throughout all phases of a software development program. It defines the role of all participating team organizations, groups, and agencies directly involved in the program. The government and contractors are provided with processes, methods, and tools that enable both organizations to better anticipate outcomes and make better decisions.

These new processes and methods can provide NHTSA with a solid foundation for introducing risk management concepts into new regulations (Ref. 22). They can also form the bases for extending industry-based recommended practices for software development system reliability. Management tools, such as TRM, can also be used to coordinate the development and eventual integration of multiple collision warning systems.

We propose that NHTSA initiate a program to review the application of these and other applicable techniques to ECBS and other safety critical onboard systems. The proposed report will detail the fundamentals of the applicable processes such as CMM, RMA, and TRM and suggest how they may be used by NHTSA as part of its R&D and regulatory processes.

11 REFERENCES

1. *Hecker, F., Hummel, S., Jundt, 0., Leimbach, D., Faye, I., and Schramm, H., "Vehicle Dynamics Control for Commercial Vehicles" Proceedings of the 1997 SAE Truck and Bus Meeting and Exposition, November 17-20, 1997.*

2. *Ervin, R., Fancher, P., Christopher, W., "Heavy Truck Stability Enhancement" Proceedings of the Third Annual Automotive Enhanced Driving / Night Vision Conference, September 16-17, 1997.*

3. *"The Seven Layer Reference Model," UNI Corporation http://bbs-win.uniinc.msk.ru/tech1/1994/osi/layers.htm.*

4. *Surface Vehicle Recommended Practice, SAE 1939/11, Physical Layer-250K bits/s, Shielded Twisted Pair*

5. *Surface Vehicle Recommended Practice, SAE 1939/21, Data Link Layer*

6. *Surface Vehicle Recommended Practice, SAE 1939/71, Vehicle Application Layer*

7. *Surface Vehicle Recommended Practice, SAE 1939/73, Application Layer - Diagnostics*

8. *Fredriksson, L.-B., "Controller Area Networks and the Protocol CAN for Machine Control Systems," Mechatronics, Vol. 4, No. 2, pp. 159-192, 1994.*

9. *"Using Fault Tree Analysis in Developing Reliable Software," Ovstedal, E.O., IFAC Safecomp '91 Trondheim Norway, 1991.*

10. *Jacobson, J., Johansson, L.-A., Lundin, M., "Safety of Distributed Machine Control Systems," Swedish National Testing and Research Institute; BorÂs, Sweden 1996 ECBS Brakes in the Rail Industry.*

11. *ANSI/IEEE "Standard Glossary of Software Engineering Terminology"*

12. *Grady, R. B. "Practical Software Metrics for Project Management and Process Improvement," Prentice Hall, Englewood Cliffs, NJ, 1992.*

13. *"Performance Prediction of the SAE J1850 and Related Buses for In-Vehicle Communications Requirements for the ITS Safety-Related User Services," prepared for DOT/NHTSA/OCAR under contract no. DTNH22-93-D-07317.*

14. *Decker, H., Wrede, J., "Brake-by-Wire Solutions, Advantages and the Need for Standardization," Bosch 1994.*

15. *Decker, H., Wrede, J., "Brake-by-Wire for Commercial Vehicles," SAE International Truck and Bus Meeting and Exposition, November, 1992.*

16. *Middleton, Dan, et al, "Assess the Feasibility of a Standardized Electronic Diagonostic Device for Maintenance and Inspection of Commercial Motor Vehicles," Texas Transportation Institute, Texas A&M University System, April 1995, Report No. FHWA-MC-97-070.*

17. *Federal Motor Vehicle Safety Standards: Air Brake Systems, U.S. Department of Transportation, National Highway Transportation Administration, 49 CFR Part 571, March 1997.*

18. *"Heavy Vehicle Air Brake Performance," National Transportation Safety Board Safety Study, Report No. NTSB/ss-92-01, April 29, 1992.*

19. *"Performance Criteria for Air Brake Component Combinations on In-Use Commercial Motor Vehicles," U.S. Department of Transportation, Federal Highway Administration, FHWA-MC-96-008, June 1996.*

20. *Surface Vehicle Recommended Practice, SAE 1739, Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) Reference Manual.*

21. *Lindemann, K., Petersen, E., Schult, M., Korn, A., "EBS and Tractor Trailer Brake Compatibility," Proceedings of the SAE Truck and Bus Meeting and Exposition, November 17-19, 1997.*

22. *Willke, T. L., Shires, T.M., Cowgill, R.M., Selig, B.J., "U.S. Risk Management Can Reduce Regulation, Enhance Safety," Oil & Gas Journal, June 16, 1997.*

A1 PROPOSED CHANGES TO FMVSS NO. 121

The following is a report supplied by the heavy duty truck manufacturers as a contribution to this task order.

Authors: Richard Hildebrandt
Paul Oppenheimer

SAE EBS Working Group
FMVSS 121 Modifications for Electronic Controlled Air Brake Systems
FMVSS 121 AIR BRAKE SYSTEMS

Re-Draft to accommodate Electronic Control of Service, Emergency and Parking Brake Systems

(Amendments and additions are in italics).

S4. Definitions

"Agricultural commodity trailer" means a trailer . ...and an arrangement of air
and/or electrical
control lines and reservoirs that minimizes damage in field operations

"Air brake system" means a system . .
mechanical components.
An Electronic Controlled Brake System (ECBS) is also considered to be an air brake system.

"Data communication" means the transfer of data.

"Electronic Controlled Air Brake System" means an air brake system that uses electronic control to transmit signals from the driver control to a compressed air system which actuates the service brakes. This definition includes full pneumatic, full electronic and combined pneumatic/electronic control systems. The emergency and parking brake systems may also use electronic control signals from the driver controls.

"Electric trailer control line" means an electrical connection between towing vehicles and towed vehicles, which provides the braking control function. It comprises the electrical wiring and the connectors and includes the parts for data communication and the electrical energy supply for the control transmission of the towed vehicle.

"Pulpwood trailer" means a trailer . . . and an arrangement of air
and/or electrical
control lines and reservoirs designed to minimize damage in off-road operations.

S5 Requirements

S5.1.2.A *Air reservoirs*

S5.1.2.B Electrical energy reservoirs (batteries)
a) In the event of a failure of the electrical energy source and starting from the nominal value of the battery energy level, as specified by the vehicle OEM, after 10 minutes of full-treadle brake application, it shall meet the requirements specified in S5.3.1

b) When the battery voltage falls below a value at which the stopping distances specified in S5.3.1 can no longer be achieved, the red brake system indicator lamp specified in S5.1.5.B shall be activated

c) After the red brake system indicator lamp has been activated, it should be possible to apply the service and parking brake controls and obtain at least the emergency braking performance specified in S5.7.1. and the parking brake performance specified in S5.6.1 or 5.6.2, respectively.

SAE EBS Working Group
FMVSS 121 Modifications for Electronic Controlled Air Brake Systems

S5.1.5.A Warning signal

A signal ..... audible and visual.
A red brake system indicator lamp as specified in S5.1.5.B may be used to satisfy this requirement.

S5.1.5.B Brake system indicator lamp

Each motor vehicle equipped with ECBS shall have one red brake system indicator lamp and if the vehicle is designed to pull trailer(s), the motor vehicle shall have another red brake system indicator lamp for the traile brake systemr, the lamp(s) mounted in front of and in clear view of the driver, which meets the requirements of S5.1.5.B(1) through S5.1.5.B(3).

S5.1.5.B(1)

The brake system indicator lamp shall be activated whenever the following conditions occur:

(a) A loss of electrical continuity (eg. breakage, disconnection) in the service brake control system (excluding the battery) such that the stopping distances specified in S5.3.1 can no longer be achieved.

(b) When the battery voltage falls below a value at which the stopping distances specified in S5.3.1 can no longer be achieved.

(c) A loss of electrical continuity (eg. breakage, disconnection) in the parking brake control system (excluding the battery) such that the performance specified in S5.6.1 or S5.6.2 can no longer be achieved.

(d) When a truck tractor without a pneumatic control line is coupled to a trailer without an electrical trailer control line. (Figure 4)

Additionally, any truck tractor with ECBS connected to a trailer with ECBS via an electric trailer control line shall activate the trailer brake system indicator lamp whenever the following conditions occur:

(e) A loss of electrical continuity (eg. breakage, disconnection) in the trailer service and parking brake control systems such that the retardation forces specified in S5.4.1 and 5.6.1or 5.6.2, respectively, can no longer be achieved.

(f) When there is an electrical failure (eg. interruption or defect in the data communication) in the electric trailer control line.

S5.1.5.B(2)

The indicator lamp shall remain activated as long as an abovementioned condition exists, whenever the ignition (start) switch is in the "on" position, whether or not the engine is running. Each message about the existence of such a condition shall be stored after the ignition switch is turned to the "off" position and automatically reactivated when the ignition switch is again turned to the "on" position

SAE EBS Working Group
FMVSS 121 Modifications for Electronic Controlled Air Brake Systems

S5.1.5.B(3)

The indicator lamp shall also be activated as a check of lamp function whenever the ignition is turned to the "on" or "run" position. The indicator shall be deactivated at the end of the check of lamp function unless there is an above-mentioned condition or a message about such a condition that existed when the key switch was last turned to the "off" position.

S5.1.6.A Antilock Brake System

S5.1.6.B Electronic Controlled Brake System (ECBS)

(a) The electric trailer control line (signal) shall transmit braking data between the tractor and trailer(s) for control of trailer(s) braking. Other information may be transferred by this line provided that the braking functions have priority and are maintained in the normal and failed modes. The transmission of other information shall not delay the braking functions.

(b) A truck tractor equipped with an electric trailer control line and no pneumatic control line shall recognize that the coupling of a trailer equipped only with a pneumatic control line is not compatible; and when the system is energized, the brakes on either vehicle shall be automatically applied, with at least the effectiveness prescribed for the parking brake performance in S5.6.1 or 5.6.2. The red indicator light (S5.1.5.B(1)(d), together with the trailer ABS malfunction light (S5.1.6.2(b)), shall warn the driver. See Figure 4.

(c) In the case of a truck tractor equipped with both pneumatic and electric trailer control lines, both control signals shall be present at the coupling head and at the connector. When such a truck tractor is connected to a trailer which is also equipped with both pneumatic and electric trailer control lines, then both signals shall be present at the trailer, and the trailer shall decide which control signal to use.

(d) A trailer may be equipped with an electric trailer control line and no pneumatic control line, provided that it can only be operated in conjunction with a towing vehicle with an electric trailer control line. Otherwise, when connected to an incompatible vehicle, the trailer parking brakes shall remain applied, or be automatically applied, and the trailer ABS malfunction light shall also be activated (S5.1.6.2(b)). See Figure 4.

(e) It must be possible to apply and release the service brakes when the ignition is switched "off", and provide a full control signal for the service braking system of the trailer. It must also be possible to apply and release the parking brake when the ignition is switched "off".

(f) Any electrical auxiliary equipment (eg. lights, wipers) shall not adversely affect the service, emergency and parking brake performance, either in normal operation or after a failure in such auxiliary devices.

SAE EBS Working Group
FMVSS 121 Modifications for Electronic Controlled Air Brake Systems

S5.1.6.2(b)

Each truck tractor manufactured.....is capable of transmitting a malfunction signal from the antilock brake system(s) on one or more towed vehicles (eg. trailers and dollies),
and ECBS failures as described in S5.1.5.B(1)(d), (e) and (f), and when a towing vehicle without an electric trailer control line is coupled to a trailer without a pneumatic control line,
to the trailer ABS malfunction lamp.....unless a trailer ABS malfunction signal is present.

S5.1.7 Service brake stop lamp switch

A switch *or signal* that lights the stop lamps...

S5.5.1 Antilock System Malfunction
....antilock system shall not increase the actuation and release times of the service *brakes beyond the requirements of S5.3.3 and S5.3.4.*

S5.6.3.1 (Parking brake system - Application and holding)

The parking brake system shall ..... are at the levels determined in S5.6.3.4.
In the case of a parking brake system with electric control, the driver shall be able to apply the parking brake with any single break in the electric wiring of the parking brake control system, and achieve the performance specified in S5.6.1 or S5.6.2, unless the parking brake is fully applied automatically. The appropriate red brake system indicator light shall also be activated (S5.1.5.B(1)(c)).

N.B. THIS FAILURE MODE ("any single break in the electric wiring of the parking brake control system") MAY ALSO BE RELEVANT TO THE FOLLOWING PARAGRAPHS DEALING WITH "any single leakage-type failure" -:
S5.6.3.3, S5.6.3.4, S5.6.5.1, S5.6.5.3, S5.6.6.1, S5.6.6.3, S5.6.6.4 and S5.6.6.6.

S5.7.1 Emergency Brake System Performance

When stopped six times ... on a road service having a PFC of 0.9, with a single failure in the service brake system
resulting from a loss of electrical continuity (eg. breakage, disconnection) in the service brake control system (excluding the battery), or
of a part designed to contain compressed air or brake fluid.....and with unlimited wheel lockup permitted at any speed

S5.7.3 Towing Vehicle Emergency Brake Requirements

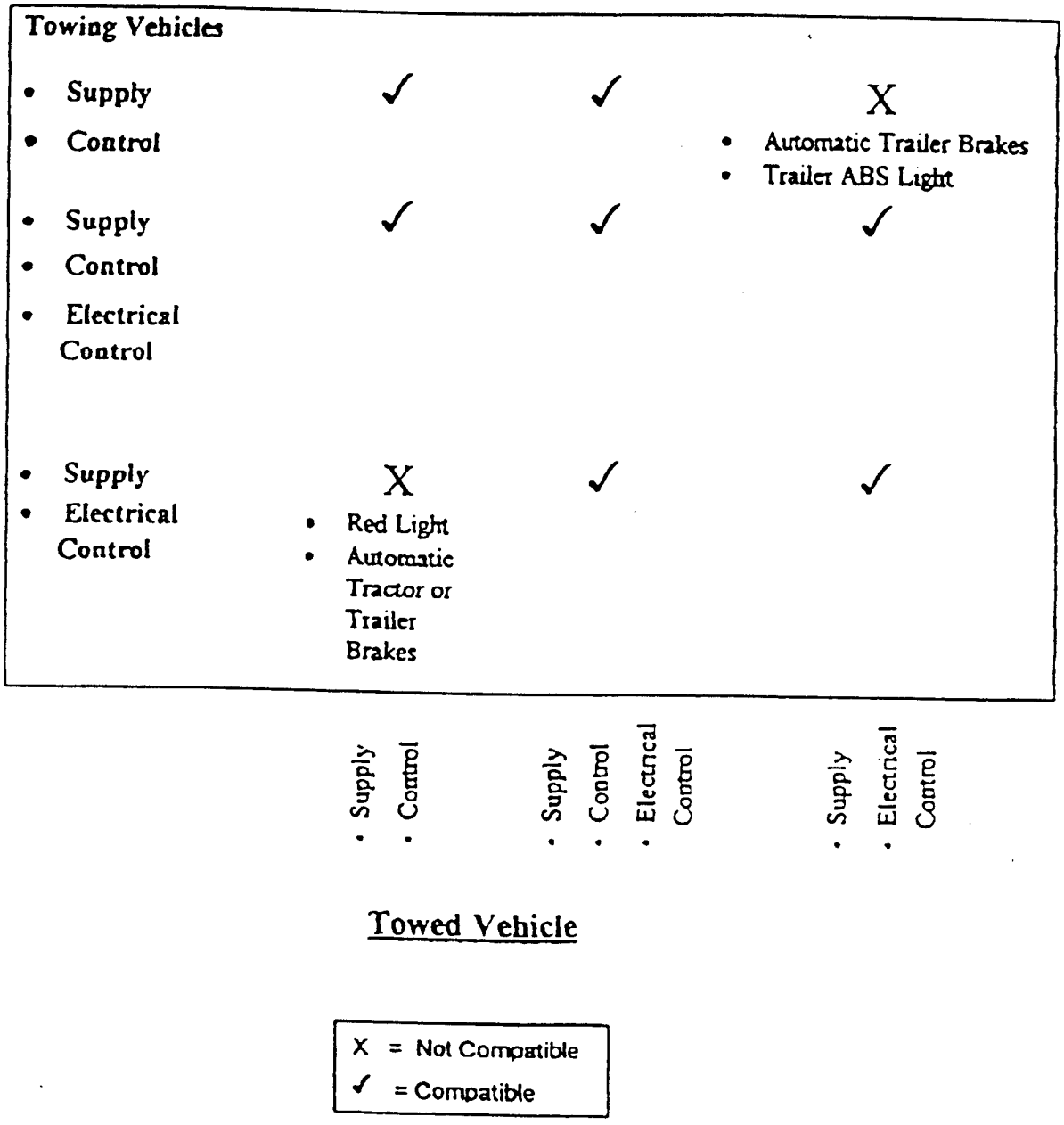
(d) In the case of towing vehicles equipped with ECBS, be capable of providing modulated control to the trailer by means of the service brake control, with a single failure in the towing vehicle service brake system as specified in S5.7.1

SAE EBS Working Group

FMVSS 121 Modifications for Electronic Controlled Air Brake Systems

Tractor-Trailer Coupling Interface

– FIGURE 4—



SAE EBS Working Group
FMVSS 121 Modifications for Electronic Controlled Air Brake Systems

BRAKE SYSTEM INDICATION LAMP OPERATION

(FIGURE 5)

S5.1.5B (Proposed)	Red (Truck, Bus, Tractor)	Red (Trailer)	Yellow (ABS) (Truck, Bus Tractor)	Yellow (ABS) (Trailer)
A. Service Brake Electrical Control	X			
B. Battery Low Voltage	X			
C. Parking Brake Electrical Control	X			
D. Tractor ECL with Trailer PCL (Fig. 4)	X	X		
E. Trailer Service and Parking Brake Electrical Control		X		
F. ECL Data Defect		X		
S5.1.6.2(b) (Proposed) Tractor ECL with Trailer PCL		X		
S5.1.6.2(b) (Proposed) Tractor PCL with Trailer ECL				X
S5.1.5.A (Current) Low Pressure	Optional			
S5.1.6.2(a) and (b)(Current) ABS Malfunction			X(a)	X(b)

Note: ECL = Electric Control Line
PCL = Pneumatic Control Line

SAE EBS Working Group
FMVSS 121 Modifications for Electronic Controlled Air Brake Systems
WARNING LIGHTS AND BRAKE PERFORMANCE AFTER ELECTRICAL 'FAILURES'
- FIGURE 6 -

SB = Service Brake Performance S5.3.1 EB = Emergency Brake Performance S5.7.1 PB = Parking Brake Performance S5.6.1or 5.6.2		WARNING LIGHT	PERFORMANCE	ECL = Electric Trailer Control Line PCL = Pneumatic Control Line COMMENTS
S5.1.2.B(b),(c) S5.1.5.B(1)(b)	Battery - Low Voltage	Red (Truck)	EB - PB	
S5.1.2.B(a)	Energy Source Failure		SB	After 10 minutes full-treadle apply
S5.7.1, S5.7.3 S5.1.5.B(1)(a)	Service Brake Electrical Failure	Red (Truck)	EB	Modulated Electronic Control to Trailer
S5.1.5.B(1)(c) S5.6.3.1	Parking Brake Electrical Failure	Red (Truck)	PB	
S5.1.6.2(b) S5.1.5.B(1)(e)	Trailer Service Brake Electrical Failure	Red (Trailer)		
S5.1.5.B(1)(e) S5.1.6.2(b)	Trailer Parking Brake Electrical Failure	Red (Trailer)	PB	
S5.1.5.B(1)(f)	Data Defect in ECL	Red (Trailer)		
S5.1.6.B (b) S5.1.5.B(1)(d)	Tractor ECL with Trailer PCL	Red (Trailer)		Automatic PB Application
S5.1.6.B (d)	Tractor PCL with Trailer ECL	Yellow ABS (Trailer)		Automatic Trailer PB Application
S5.1.6.B (e)	Ignition Switch "Off"		SB - EB - PB	
S5.1.6.B (f)	Auxiliary Electrical Equipment (including failure)		SB - EB - PB	No Adverse Effects

A2 AAR SPECIFICATION S-4200

Specification S-4200

PERFORMANCE REQUIREMENT FOR TESTING ELECTRICALLY CONTROLLED PNEUMATIC CABLE-BASED (ECP) FREIGHT BRAKE SYSTEMS

Adopted: May, 1997

1.0 PURPOSE

The overall objectives of this specification are:

1. Assure that the performance of electrically controlled pneumatic (ECP) freight brake systems is uniform and consistent among equipment from different manufacturers.

2. Assure that cars equipped with AAR approved ECP brake systems from different manufacturers can be operated together in any electrically braked train.

3. Assure that AAR approved electric brake systems meet a high standard level of safety and reliability.

2.0 SCOPE

This specification defines the requirements for an AAR approved freight train power brake using electrically controlled freight brake systems suitable for service in all-electric braked trains. Operation of such systems in a conventionally braked train is covered by AAR Specifications S-461, S-462, S-464 and S-467.

2.1 Definitions

2.1.1 Electrically Controlled Pneumatic (ECP) Brake System

A train power braking system operated by compressed air and controlled by electrical signals originated at the locomotive for service and emergency applications. The brake pipe is used to provide a constant supply of air to the reservoirs. Graduated release and re-application must be available. The system responds appropriately to undesired separation or malfunction of hoses, cabling, or brake pipe.

2.1.2 Car Control Device (CCD)

The CCD is an electronic control device which replaces the function of the pneumatic service and emergency portions during electric braking and provides for electrically controlled service and emergency brake applications. The CCD interprets and acknowledges the electrical signals and

controls the reservoir charging, and the service and emergency braking functions on the car. It will also send a warning signal to the locomotive in case any of the components cannot respond appropriately to a braking command. Each CCD has a unique electronic address that is keyed to car reporting marks and numbers.

2.1.2.1

In order to aid in system diagnostic services, the CCD will be able to measure the communication signal level at its interface to the communication media. The CCD will make this measurement with a resolution of ±0.05 Volts RMS. The signal measuring circuitry will have an impedance of no less than 20,000 ohms in the frequency band of 100kHz to 450kHz. The hardware which provides this measurement should have no adverse effect on the communication signal. It is recommended that this measurement be made on the low voltage side of the CCD coupling circuit.

2.1.3 Head End Unit (HEU)

Brake system control device used by the locomotive engineer to control the electric brake system. The specific functions of the HEU are:

- Provide man/machine interface to operate the ECP brake system, either directly or through a Locomotive System Integration (LSI) interface.

- Provide a data display to the engineer.

- Provide controls which allow the engineer to make the following brake commands with one movement:

  Minimum service (15% application)
  Full service (100% application)
  Emergency (120% application)
  Full release
  Graduate application and release in 1% increments

- Monitor the End of Train (EOT) beacon.

- Provide a means to turn off train line power whenever communication with the EOT is not established and during operation in switching mode.

- Provide a means to supply a two-second power application to "wake up" CCDs in a sleep mode.

- Provide mechanisms to conduct ECP brake system initial terminal test.

2.1.4 Overlay Brake System

An ECP brake system which is capable of operating in a conventionally braked train. A failure to the ECP brake system operating as an overlay system would enable a train to continue to

operate as a pneumatically braked train when the ECP system is turned off. An electrically braked train must come to a complete stop before the ECP system can be turned off and train operation continued with the pneumatic brake. An overlay system and a pure ECP system must operate identically as specified below when operating in the electric mode.

2.1.5 Penalty Brake Application

An automatic electric emergency brake application made by the HEU when the locomotive engineer does not respond to a warning. A penalty brake application must remain in effect for 120 seconds and until the cause for the penalty application is eliminated and the brake command is 100%.

2.1.6 End Of Train Device (EOT)

The EOT will contain a means of communicating with the HEU, a brake pipe pressure transducer and a battery which will charge off the train line cable. The EOT will act as the last node in the train and will transmit a status message once per second. The status message will consist of the current brake pipe pressure which will be displayed on the HEU. The EOT will not need an emergency brake pipe vent valve, so the hose to the EOT can be as small as, but no smaller than, 3/8" i.d. The EOT will also contain the electric train line termination circuit. The EOT must be connected to the network and must be transmitting status messages to the HEU before the train line power can be energized. The EOT must also have a flashing red warning light in accordance with FRA regulations.

2.1.7 Recovery from Intentional Non-Pneumatic emergency

An HEU emergency command must remain in effect for 120 seconds, after which the engineer must initiate a full service application.

3.0 PERFORMANCE SPECIFICATIONS

This section will describe the performance requirements for an ECP brake system. The electric brake system must function independently, and must not require the retention of the present service and emergency control valve portions. The brake system must include the following functions:

- Graduated brake applications and releases
- Continuous reservoir charging
- Pneumatic emergency back-up

3.1 ECP System Operation

The brake system is to operate as defined in the enclosed system flow charts and fault tree. The system flow chart describes the high level logic for the ECP system operation and identifies the major system functions and operational modes.

3.1.1 Train Brake Commands

The train brake commands (TBC) which determine the level of brake application for electrically controlled brake systems will be expressed as a percentage from 0 to 100% of the

maximum full service braking force in 1% increments. The brake pipe pressure setting will determine the maximum full service brake cylinder pressure as shown in Table 1 and according to the following formula;

$$P_{BC} = 0.711 * P_s$$

These pressures are for cars loaded to 100% gross rail load.

3.1.1.1

Brake cylinder pressure tolerance will be ±2 psi. An initial command during the initialization of the train brake system will set each CCD to the full service brake cylinder pressure setting.

3.1.1.2

Emergency command will result in a brake cylinder pressure which is 120% of the full service brake cylinder pressure setting with a tolerance of ±2 psi (Table 1).

3.1.1.3

Minimum service application will be a 15% brake application. Once a minimum service application is made, it must be possible to reduce the brake application in 1% increments.

3.1.1.4

The HEU brake controller must provide the engineer a means for requesting;

a. Direct brake release
b. Graduated brake release
c. Graduated service brake application
d. Full service brake application
e. Emergency brake application

TABLE 1 - MAXIMUM FULL SERVICE BRAKE CYLINDER PRESSURES, LOADED BRAKE RATIOS AND EMERGENCY B.C. PRESSURES

3.1.2 Brake Cylinder Pressure Control for Empty or Partial Load Conditions

3.1.2.1

The CCD must be designed such that the brake cylinder pressure for any application is reduced in proportion to the percentage of gross rail load. The percentage GRL for any car is determined by a message from the HEU during system initialization or by a load weighing device on the car. This percentage GRL is locked into the CCD memory every time the train brake system is initialized during the initial terminal air brake test or when the load condition of the train is changed. On those cars equipped with on-board load sensing equipment for conventional operation, the empty/load condition information from the HEU will take precedence when the car is operated in an electrically braked train. If the car is equipped with a proportional empty/load device, then the data from that device will take precedence over the information from the HEU.

When the brake system is initialized during the initial terminal inspection or at another location where the train is loaded or emptied, the car is told what its' percentage of gross rail load is, either by a message from the HEU or by an on-board self weighing device.

The CCD will provide the brake cylinder pressure necessary to keep the loaded and partially loaded car brake ratio no higher than 12.8% of gross rail load at a 90 psi brake pipe pressure under most load conditions. The loaded brake ratio will vary depending on the brake pipe pressure (see Table 1). The CCD will determine the brake cylinder pressure based on formulas and limits shown below. Note that the empty car brake ratio may be greater than 12.8%.

3.1.2.2 Full Service Brake Cylinder Pressure

The CCD can use the following procedure to compute the maximum brake cylinder pressure for its particular car loading. Note that this pressure will be less than or equal to the loaded brake cylinder pressure given in section 3.1.1, Train Brake Commands.

$$P_{BC\,MAX} = (NBR * W) / C$$

Where NBR = $0.128 * BPP / 90$

BPP = Operating brake pipe pressure

C = $(A_P * LR * EFF)$

A_P = Area of the B.C. piston(s)

LR = Lever ratio

EFF = Measured rigging efficiency @ 64.0 psi brake cylinder pressure

W = Total car weight at initial terminal

P_{BC} = Maximum brake cylinder pressure for the cars' current %GRL

The constant C is programmed into the CCD only once when it is installed on a particular car. The constant C remains unchanged as long as a particular CCD remains with its car. The CCD must have the software capability to be adjusted by the car builder for the constant C.

3.1.3 Pneumatic Emergency Back-up

Each CCD will provide the means to pneumatically (without requiring electrical power) apply emergency brake cylinder pressure if the brake pipe pressure falls below 40 psi. A pneumatically controlled brake pipe emergency vent valve will be optional on pure ECP cars, and required on cars equipped with overlay systems per AAR S-401, section 2.3. On operating CCDs, electric operation will take precedence over pneumatic operation, even if the brake pipe pressure falls below 40 psi. Once the brake pipe pressure exceeds 40 psi, or when the ECP system is operating, a means shall be provided to release emergency brake cylinder pressure.

3.1.4 Switching Mode

A means must be provided to allow operation of the ECP system when the EOT is not communicating with the HEU or when the train is separated during road switching operations. All modes of failure operation will be suspended when operating in switching mode with the exception of loss of communications and loss of brake pipe pressure. Loss of communications will be handled as outlined in 3.3.2.1.1 for cars cut off from HEU brake commands, but the HEU will ignore any lack of EOT status messages. Loss of brake pipe pressure will be handled as outlined in 3.3.2.2.5. Operation in switching mode cannot exceed 15 minutes and train speed cannot exceed 20 mph. If 20 mph is exceeded, a penalty electric emergency brake application must occur. If the 15 minute time period is exceeded, the engineer must be warned. If he does not reset the HEU for switching mode within 6 seconds, a penalty electric emergency brake application must occur. Switching mode must be selected prior to separating the train. Cars left standing without communication with the HEU will make an electric emergency application when three consecutive brake commands are missed. The electric emergency must be maintained on standing cars for at least one hour until communications with those cars and the HEU is reestablished.

NOTE: Brake pipe pressure must be vented to atmosphere on any standing cars. Then, if the CCDs time out after one hour and go into the sleep mode, the pneumatic emergency backup will keep the brake applied.

3.1.5 Automatic Brake Cylinder Venting

A means shall be provided to automatically vent brake cylinder pressure on an arriving train, either with the road locomotives before they are cut off from the train, or with a portable hand-held device. Head end power must not be required to accomplish this task. Use of switching mode prior to engaging automatic brake cylinder release will remove the need to use an EOT during this operation.

3.1.6 Inadvertent Use of the Pneumatic Brake

Whenever the ECP system is energized, and the ECP system is not in electric emergency, movement of the automatic brake valve handle to any position in the service application zone, must result in an audible and visual warning to the engineer stating that the automatic brake valve handle was used in error. If the engineer does not respond to the warning within six seconds by returning the automatic brake valve handle back to release position, an ECP penalty emergency application must occur.

3.2 Messaging Requirements

3.2.1 Brake Commands

A train brake command (TBC) will be transmitted by the HEU once per second. The TBC will be a priority message. The TBC will be a percentage of full service braking force. 0% will be release, 15% will be minimum service, 100% will be full service and 120% will be emergency. Each TBC will include a status query for an individual CCD. Each CCD will be queried on a round robin basis until all CCD have been queried, then the process will repeat.

3.2.2 EOT Status Messages

The EOT will transmit a status message once per second. The status message will contain the brake pipe pressure which will be displayed on the HEU. The EOT message will be a priority message.

3.2.3 Individual Car Status Messages

Each CCD will respond to the appropriate status query by transmitting the brake pipe pressure, the brake cylinder pressure, the reservoir(s) pressure, the battery voltage, the CCDs cut-in/cut-out status, and other information as identified in the Intra-Train Communications Specification. This information will not be displayed on the HEU but will be stored in an event recorder. This will not be a priority message.

3.2.4 Exception Messages

A CCD, and the EOT where applicable, will broadcast an exception message on the network for any of the following conditions:

- Improper brake cylinder pressure
- Failure of brake pipe to charge (EOT only)
- Brake pipe pressure below 50 psi (also EOT)
- Reservoir pressure below 50 psi
- Loss of communications (also EOT)
- Low battery voltage just prior to taking itself off line

3.2.4.1

When a CCD experiences multiple faults, only the more serious fault will initially be reported and acted upon. Once the more severe fault is cleared then the lower priority faults will be acted upon. The hierarchy of fault severity is shown in Table 2.

3.2.4.2

When the HEU has commanded an emergency brake application, either penalty or intentional, a CCD must suppress all exception messages except loss of communications. Normal exception messages can resume only after the system has recovered from the emergency application as described in sections 2.1.5 and 2.1.7. Exception clear messages will be allowed when the HEU is commanding an emergency.

TABLE 2 - ECP BRAKE SYSTEM FAULT HIERARCHY

Fault Degree	General Fault Description	Examples
First Degree Fault (Most Severe)	CCD is unable to communicate with HEU. Independent action must be taken.	• Failure in network continuity. • CCD transceiver failure.
Second Degree Fault	A fault which affects the entire system occurs, but CCD is still in communication with HEU. The CCD will receive instructions from HEU.	• Loss of brake pipe pressure.. • Less than 85% operable bakes.
Third Degree Fault	A fault local to a CCD which requires the CCD to go offline occurs. If possible the CCD reports the fault to the HEU. The HEU will log the CCD as "inoperative."	• Low CCD battery voltage. • Etc.
Fourth Degree Fault	A fault local to a CCD which does not require the CCD to go offline occurs. The fault is reported to the HEU.	• Low reservoir pressure. • Low brake cylinder pressure. • High brake cylinder pressure. • Etc.

3.2.5 Control Messages

- CCD cut out
- Switching mode on or off
- Train initialization and serialization commands
- Yard train automatic brake cylinder release

(Other messages concerning car health monitoring and distributed locomotive control are covered in the Intra-Train Communications Specification.)

3.3 System Operation

3.3.1 Initial Terminal Test

Note that the following describes the requirements for the initial terminal brake system test, and is treated separately from any required safety appliance or running gear inspections.

3.3.1.1 Train Make Up Procedures

The EOT must be connected to the last car, and all cables must be connected completing a circuit, before train line power can be energized.

3.3.1.2

The remaining test procedures are shown in the attached Terminal Test flow chart.

3.3.2 Failure Modes

These failure modes are for pure ECP or overlay operation.

3.3.2.1 Signal Transmission Failure

Signal transmission failure is defined as a total failure of the entire electric brake control network, such that communication to and/or from the last car is broken at some point in the train.

3.3.2.1.1 Single or Multiple Breaks in the Communications Network

If any CCD (and the EOT) determines that it has missed three consecutive HEU beacons, it will maintain the current brake application and transmit a "loss of signal" message. If that CCD subsequently receives a "loss of signal" message from any other CCD or the EOT within one second, then that CCD will assume that the entire communications link is broken and must make an electric emergency brake application. If that CCD does not receive a "loss of signal" message from any other CCD, it will cut itself out with the brake cylinder connected to atmosphere per Para. 3.3.2.2.2. The HEU must detect the failure when three consecutive EOT status messages are missed. The HEU must then transmit an electric emergency brake application command to all CCDs still in communication with the HEU.

3.3.2.1.2

The locomotive engineer must be given an audible and visible warning of network failure, and an electric emergency application must be made. Emergency application on the cut off cars must be held for one hour, after which the pneumatic emergency will maintain the application as the CCDs time out and enter a "battery conservation" mode.

3.3.2.1.3

In the event of train line communications failure, the system will return to normal operation when the HEU receives three consecutive EOT messages after the train has come to a stop per Para. 2.1.5.

3.3.2.2 Individual Car Control Device Failure

Individual car control device failure is defined as the failure of any one CCD to respond appropriately to commands from the HEU.

3.3.2.2.1 Incorrect Brake Cylinder Pressure

If the brake cylinder pressure monitored by each CCD does not correspond correctly ($\pm$5 psi) with the brake signal command after allowing for the build up time or release time, a 15 second

settling period and after correcting for any empty or partially loaded brake cylinder pressure, the locomotive engineer must be given a warning of the failure, and must be informed of the location in the train of the defect. The locomotive engineer must have the option of allowing the defective brake system on that car to continue to operate.

3.3.2.2.2 Local Signal Failure

If the signal to an individual CCD should fail for any reason, that CCD would not receive any brake commands. When three consecutive brake commands have been missed, that CCD would attempt to broadcast a "loss of signal" message, but would be unable to do so. After the fifth brake command has been missed, that CCD would "go to sleep" with the brake cylinder connected to atmosphere. The locomotive engineer must be given a warning that communication with that CCD has failed when the status message from the HEU to that CCD is not answered (see Para. 3.2.1 and 3.2.3), and must be informed of the location in the train of the defective CCD. If at a later time the CCD begins receiving the HEU beacons and has no other faults, it will cut itself in and continue to operate normally. The HEU will inform the engineer that the CCD is back on line if it receives a response from that CCD during a normal polling message.

NOTE: If the failure occurs on a car equipped with an overlay system, that car may have to be cut out pneumatically in order to prevent stuck brakes. Stuck brakes can occur when the pneumatic system on an overlay car reacts to small pressure changes in the brake pipe when the rest of the train is operating in ECP mode.

3.3.2.2.3 Local Transceiver Failure

Communication within the entire network may be disrupted if the transceiver in an individual CCD, or any other ECP brake system component, fails to a noise generating mode. A means must be provided to detect and disable a noise generating transceiver within two (2) seconds of the initial occurrence of the failure.

3.3.2.2.4 Loss of More Than 15% of CCDs in Train

If communication to more than 15% of the CCDs in any train fails for any reason, or if more than 15% of the CCDs are cut out by the locomotive engineer, the locomotive engineer will be given an audible and visual warning. The locomotive engineer must then take action to apply the brakes or increase a current brake application in order to reduce the speed of the train. If the locomotive engineer takes no such action after a 6 second period, a penalty emergency brake application must occur.

3.3.2.2.5 Brake Pipe Blockage

If the brake pipe becomes blocked, restricted, or an angle cock is closed, the locomotive engineer must be given an audible and visual warning that the reservoirs behind the blockage are not being charged. After a brake application is made, the EOT will wait 15 seconds, then start a three minute timer. If the brake pipe pressure has not increased by at least 2 psi in 3 minutes, the EOT will send a warning to the HEU.

3.3.2.2.6 Brake Pipe Separation

If the brake pipe breaks or separates, each CCD and the EOT must transmit a "loss of pressure" message to the HEU when the brake pipe pressure is at or below 50 psi. When the HEU receives three consecutive "loss of pressure" messages from at least three separate cars within ten seconds, HEU transmits a penalty electric emergency brake application command. NOTE: In the case of a train break-in-two, the train may also be initiating an electric emergency brake application due to signal loss (see para.3.3.2.1.1).

3.3.3 Recovery from Emergencies

In all cases, an ECP emergency has to stay in effect for 120 seconds. Recovery cannot be made until the 120 second time period has elapsed.

CAUSE	RECOVERY PROCEDURE
Low B.P. pressure (3.3.2.2.6)	After the 120 second time period, any three CCDs reporting B.P. pressure of 60 psi or higher will start a 60 second timer. After 60 seconds, the engineer may command a full service application. If the B.P. pressure is at least 60 psi at all reporting CCDs, then the system returns to normal operation. If there are still at least three CCDs in the train reporting lower than 50 psi B.P. pressure, these CCDs will again initiate an emergency application. The engineer will then have to wait 120 seconds and repeat the recovery process. If the recovery is still unsuccessful, a serious leak still exists in the train. This recovery procedure is identical in either switch or run mode.
Loss of communications (3.3.2.1)	After the 120 second waiting period, and after the break in the communications line has been repaired, the system will return to normal operation when the HEU receives the EOT beacon. At that point a full service application will restore the system to normal operation. If the communications break cannot be repaired, and the train must be moved in switch mode to a siding, the CCDs behind the communications break which are in emergency will release when the brake pipe pressure is reduced by 15 to 35 psi and held for 30 seconds.
Inadvertent use of the pneumatic brake	After the 120 second waiting period, a full service brake application will return the system to normal operation.
Percentage of operative brakes falls below 85%	After the 120 second waiting period, the train may be operated in switch mode to set out enough defective cars to return to at least 85% operative brakes. The system must be re-initialized to return to normal operation.

Switching mode time or speed exceeded	After the 120 second waiting period, reset the system to switch mode.

4.0 PERFORMANCE TESTS FOR SINGLE CAR BRAKE EQUIPMENT

These tests will be made on an AAR approved single car test rack. Initialize the CCD as follows;

C	=	572	BPP	=	90 psi
GRL	=	286,000 lbs	Lt. Wt	.=	43,000 lbs

This will result in the following target brake cylinder pressures for different load conditions as shown in table 3;

TABLE 3 - TARGET BRAKE CYLINDER PRESSURES

% TBC	100% LOAD	50% LOAD	EMPTY
0	0	0	0
10	6.4	6.4	6.4
15	9.6	9.6	9.6
20	12.8	11.2	10.2
30	19.2	14.4	11.4
40	25.6	17.6	12.7
50	32.0	20.8	13.9
60	38.4	24.0	15.1
70	44.8	27.2	16.3
80	51.2	30.4	17.6
90	57.6	33.6	18.8
100	64.0	36.8	20.0
120	76.8	44.2	24.0

The following tests 4.1 through 4.4.1 are to be conducted at 100% load, then repeated at 50% load and 0% load.

4.1 Minimum Service Requirements

4.1.1 Application Test

Make a minimum service electric brake application (15% brake application). Final brake cylinder pressure should be 9.6 $\pm$ 2 psi in no more than 2.0 seconds

4.1.2 Release Test

Release from a minimum service application. Brake cylinder piston must fully retract into the cylinder.

4.2 Full Service Requirements

4.2.1 Application Test

Make an electric full service brake application (100% brake application). Brake cylinder pressure must build up to the pressure listed in Table 3 ±2psi in no more than ten seconds.

4.2.2 Release Test

Release the electric full service brake application. Brake cylinder pressure must reduce from full service brake cylinder pressure to 5 psi or less in no more than 15.0 seconds.

4.2.3 Graduated Release Test - Application

With the auxiliary reservoir fully charged, make an electric full service brake application (100% brake command) and hold for 10 seconds.

4.2.4 Partial release Test

Make a partial release to a 40% brake command. Brake cylinder pressure is to be in accordance with Table 3 ±2psi. Hold for one minute.

4.2.5 Application After Partial Release Test

Make an electric full service application (100% brake command) and hold for 10 seconds. Brake cylinder pressure must be in accordance with Table 3 ±2psi. At the completion of this test, fully release the brake application.

4.3 Electric Emergency Requirements

4.3.1 Emergency Application Test

Immediately after the brake release in Para. 4.2.5, make an electric emergency application (120% brake application). Emergency brake cylinder pressure build-up time from 0 psi to pressure listed in Table 3 ±2psi will be no more than 10 seconds.

4.4 Graduated Application and Release Requirements

4.4.1 Graduated Application and Release test

Make a minimum service application (15% brake command). Reduce the brake command to 10%, then make brake applications in increments as shown in Table 3 up to a full service application, then release the brakes by the same increments. Wait five seconds between each application and release. Brake cylinder pressure at all brake commands must correspond to the limits listed in Table 3 with a tolerance of ±2 psi.

5.0 PERFORMANCE TESTS ON 150-CAR TEST RACK OR TRAIN

These tests will be made on an AAR approved 150 car test rack or an equivalent train. The test rack or test train shall consist of at least 150 operative brakes with a minimum of 50 feet of brake pipe per brake for a minimum total of 7,500 feet of brake pipe. Brake cylinder piston travels must be at the maximum allowable limits. All CCDs will be initialized as follows;

C	=	572
BPP	=	90 psi
GRL	=	286,000 lbs
Lt. Wt.	=	43,000 lbs

The following tests are to be conducted at 100% load.

NOTE: A dummy speed signal will have to be provided in order to recover from any electric emergency or penalty applications resulting from the following tests. Penalty electric emergency applications must be held until the train speed is zero. The speed signal will also be necessary when testing in switching mode.

5.1 Charging Test

5.1.1

Start test with all reservoirs drained to atmospheric pressure. With the brake pipe feed valve set at 90 psi, charge the brake pipe. Main reservoir must never fall below 110 psi during this test.

5.1.2

The reservoirs on the last car must be pressurized to 90 psi in no more than 55 minutes.

5.2 Graduated Application and Release Requirements

5.2.1

Fully charge the brake system until the reservoirs on the 150th car are pressurized to at least 85 psi.

5.2.2

Make a minimum service application (15% brake command). Reduce the brake command to 10%, then make brake applications in increments as shown in Table 3 up to a full service application, then release the brakes by the same increments. Wait five seconds between each application and release. Brake cylinder pressure at all brake commands must correspond to the limits listed in Table 3 with a tolerance of ± 2 psi.

5.3 Repeated Full Service Brake Applications

5.3.1

With the brake system on the last car charged to at least 85 psi, make a full service brake application. When the brake cylinder pressure of the first car reaches 64.0±2psi, record the brake cylinder pressure on the last car, then fully release the brake.

5.3.2

When the brake cylinder pressure begins to release on the last car, wait fifteen seconds, then make a full service brake application. The brake cylinder pressure on the last car must match the brake cylinder pressure recorded previously within ±2 psi after waiting 15 seconds.

5.4 Failure Mode Tests

These tests will be made under the test conditions described in Section 4.0 (150-car rack tests or equivalent train).

5.4.1 System Loss of Communications

Disconnect the signal (but not the power if cable powered) from the train. The system must give an audible and visible warning of total control network failure. An electric emergency brake application must be initiated simultaneously on all cars in not more than four seconds from the time of signal disconnection. Wait for at least 1 hour. The brakes on the disconnected CCDs must remain applied for at least 1 hour, and then they must go into a battery conservation mode within the following five minutes. At the conclusion of this test, reinitialize the system.

NOTE The release is intended to verify that a car set out at a siding will enter the "battery conservation or sleep" mode within the time specified in order to save the battery. If the brake pipe pressure was less than 40 psi, the brake would be maintained by the pneumatic emergency feature.

5.4.1.1

Repeat the test in 5.4.1, but open the brake pipe to atmosphere after the brakes apply due to communications loss. When the disconnected CCDs time out after the 1 hour waiting period, the brakes must remain applied with the pneumatic emergency back up. At the conclusion of this test, recharge the brake pipe and reinitialize the system.

5.4.2 Loss of Communications at Multiple Locations

Reconnect the signal, recharge the reservoirs to at least 85 psi, then simultaneously break the signal between cars 50 and 51, and between cars 149 and 150. All three sections must make a simultaneous emergency brake application within 4 seconds of the communications break. Reconnect the signal so that communications with the EOT is regained. After the emergency has been in effect for one minute, make a full service application. The HEU must not respond, and the emergency must stay in effect. After the emergency application has been in effect for at two minutes, make a full service brake application. The system must then return to normal operation.

5.4.3 Loss of Communications to a Single CCD

Make a 100% (full service) brake application and wait for at least 8 seconds. Break the communications path to the CCD on one of the cars. The brakes on that car must begin to release within six seconds.

5.4.4 Loss of Train line Power

Reconnect the signal, release and recharge the brake system, and disconnect the power, but not the signal, from the cable. The system must give an audible and visible warning of total power failure. The system must continue to operate on battery power for at least 15 minutes. Cut out 16 CCDs (10.7%). The HEU must command a penalty emergency brake application. After waiting 2 minutes, re-connect the cut out CCDs.

5.4.5 Brake Cylinder Leakage

Reconnect the power, then disable any one CCD in the consist by opening a brake cylinder pipe to atmosphere. Make a 15% brake application. After a 15 second waiting period, the system must give the engineer a warning of the low brake cylinder pressure, indicate the brake cylinder pressure and indicate the location in the train of the defect. Close the brake cylinder pipe opening and release the brake.

5.4.6 Excessive Brake Cylinder Pressure

5.4.6.1

Make a 15% minimum service brake application. With the 15% brake command in effect, connect brake pipe pressure, reservoir pressure or some other higher air pressure source to brake cylinder pressure on any one CCD. After a 15 second waiting period, the system must give the engineer a warning of the high brake cylinder pressure, indicate the brake cylinder pressure and indicate the location in the train of the defect. The CCD controlling that brake cylinder **must not** release the brake. Remove the high pressure air source at the completion of this test..

5.4.7 Intentional CCD Cut Out

With the 15% brake command still in effect, send a command from the HEU which will electrically cut out an individual CCD. The brake cylinder pressure on the that CCD must reduce to atmospheric pressure. Make a full service brake application. The cut out CCD must not respond.

5.4.8.1 Less Than 85% operative

Release the brake. Send a command from the HEU to cut out another 21 CCDs spaced at random throughout the train to simulate a number of defective or intentionally cut out CCDs (this assumes that the CCD cut out in 5.4.7 is already cut out. The total number of CCDs needed to be cut out for this test is 22) The HEU should give an indication that 14.7% of the CCDs have been cut-out.

5.4.8.2

Cut out one more random CCD, which increases the total number of cut out CCDs to 23 (15.3%). The system must give an audible and visual warning in not more than two seconds that more than 15% of the CCDs are inoperative. Six seconds after the warning a penalty electric emergency brake application must occur. At the completion of the test cut in all CCDs and release the brake.

5.4.9 Loss of Brake Pipe Pressure

Close the angle cock between cars 100 and 101 and partially open the angle cock at the rear of the train so that the brake pipe pressure is reduced at a service rate. A pneumatic emergency must not occur. The locomotive engineer must be given an audible and visual warning of loss of brake pipe pressure when the pressure on any three CCDs falls below 50 psi, and an electric emergency application must be initiated on all cars within two seconds of the warning.

5.4.9.1 Recovery from Emergency due to Loss of Brake Pipe Pressure

Recover from the penalty application is described in section 3.3.3.

5.4.10.1 Switching Mode

With the last car charged to at least 85 psi, make a full service (100% brake command) application. Switch the system over to switching mode. Close the angle cock and disconnect the signal between cars 50 and 51. The brakes on cars 51 through 150 must apply in emergency, while the brakes on cars 1 through 50 remain at full service. Release the brakes. After a fifteen minute time period, the HEU must give a warning that the switching mode time has expired. Do not reset the HEU for switching mode. The HEU must make a penalty electric emergency application on the first 50 cars within six seconds of the warning. Continue waiting for a total of 1 hour. The brakes on the last 100 cars must remain applied in emergency. The brakes on the first 50 cars must remain applied in emergency. After the expiration of the 1 hour waiting period, the brakes on the last 100 cars must release. Open the brake pipe on the last car to atmosphere. The brakes must reapply on each car when the brake pipe pressure at that car is reduced to 40 psi or less.

5.4.10.2

Repeat 5.4.10.1, but when the HEU warns of switching mode time-out, reset the HEU for switching mode. The brakes must stay released on the first 50 cars, and remain applied on the last 100 cars.

5.4.10.3

Repeat the test conditions in 5.4.10.1, but after the simulated train separation is made and the first 50 cars have released their brakes, increase the dummy speed signal to simulate 21 mph. The first 50 cars must immediately apply a penalty electric emergency brake application.

6.0 GENERAL REQUIREMENTS FOR ELECTRIC BRAKE INSTALLATIONS ON INDIVIDUAL CARS

6.1 Manual Brake Cylinder and Reservoir Venting

A method to manually vent brake cylinder pressure and reservoir pressure must be available at every CCD location from both sides of the car. The method of brake cylinder pressure venting must require no more than three seconds per car. It must be possible to vent the brake cylinder pressure independently of the reservoir pressure.

7.0 ENVIRONMENTAL TESTS

7.1 Vibration and Shock Environment

The CCD shall be designed and mounted on the base structure of the car to withstand continuous vibrations, in the three major axes, of 0.4 g RMS with a frequency content from 1 Hz to 150 Hz, containing peak values of ± 3 g in the 1 Hz to 100 Hz bandwidth. The CCD and its mounting shall also be designed to withstand a longitudinally oriented shock impulse (half sine wave) of 10 g peak with a ramp time of 20 msec to 50 msec. If the CCD is mounted on the car strength members (ribs, slope sheet support columns, etc.), then the bracket and mounting arrangements, together with the electronics packaging, shall be designed to provide protection from the amplification effects of any local vibration resonances. It should be noted that peak resonant acceleration levels in excess of 15 g in the 100-150 Hz range and values in excess of 50 g in the 200-500 Hz range have been measured on car strength members as a result of shock impulses sustained during yard impacts.

7.2 Temperature and Humidity tests

7.2.1

Mount the CCD on an AAR approved single car test rack or an approved equivalent. Use an outside air source at ambient temperature to charge the brake system. Place the test rack and a suitable air source in an environmental chamber. Do not use air driers. Soak the equipment at -50±2°F for 24 hours

7.2.2

After the equipment has soaked at -50±2°F, repeat the tests described in Para. 4.4.1. The CCD must meet all of the requirements outlined in Para. 4.4.1.

7.2.3

Repeat test described in Para. 7.2.1 and 7.2.2 at temperature of 150±2°F.

8.0 APPROVAL PROCEDURE

8.1

The manufacturer will apply in writing to the Director, Technical Committees-Quality Assurance, Mechanical Division, Association of American Railroads, 50 F Street NW, Washington,

DC, 20001, to initiate the approval process. This application for approval will include a description of the product and its intended use.

8.2

It is the manufacturers obligation to establish that the ECP equipment will comply with, and satisfactorily function, per this performance specification, and to the Intra-Train Communications Specification as witnessed by representatives of the AAR.

8.3

If the ECP equipment being offered is designed to emulate the performance of conventional pneumatic control valves in conventional trains, the ECP equipment must also pass the following AAR specifications.

8.3.1

"Performance Specifications For Single Capacity Freight Brakes." AAR Standard S-461.

8.3.3

"Performance Testing Procedure For Freight Brakes On A 150-car Test Rack." AAR Standard S-464.

8.3.5

"Performance Testing Procedure For Control Valve Applied to Single Car Rack." AAR Standard S-466.

8.4

The testing as described in this specification and the testing for "emulator" ECP equipment as outlined in Para. 8.3 must be performed on AAR certified test racks certified according to the following.

8.4.1

"Specifications For Freight Brake 150-car Test Rack." AAR Standard S-463.

8.4.2

"Specification For Freight Brake Single Car Test Rack." AAR Standard S-465.

8.5

ECP brake components for single car tests must be selected from a production lot of not less than 50 car sets of equipment. ECP components for 150-car rack testing must be selected from a production lot of not less than 200 car sets of equipment. All test samples will be selected by an AAR representative.

8.6

Results of all required tests will be provided by the manufacturer and furnished free of charge to the AAR for evaluation.

8.7

After the AAR examination of the ECP brake equipment and supporting information, the AAR will notify the manufacturer or supplier as to whether the product has been given a conditional approval or has been disapproved.

A3 AAR SPECIFICATION S-4210

Specification S-4210

PERFORMANCE SPECIFICATION FOR ECP BRAKE SYSTEM CABLE, CONNECTORS AND JUNCTION BOXES

Adopted May, 1997

1.0 PURPOSE

To establish the qualification test procedure for an electric brake trainline connector, cable and end-of-car junction box. The qualification test procedure is intended to verify that the designed components have high reliability, will withstand harsh environmental conditions, and have a minimum of an 8 year operating life.

2.0 SCOPE

This standard applies to ECP Brake System power and signal cable intended for use on interchange freight cars and locomotives equipped with AAR approved ECP brake systems.

2.1 Referenced Documents

ASTM B-8	Standard Specification for Concentric Stranded Copper for Electrical Conductors.
ASTM B-33	Tinned Soft or Annealed Copper Wires
ASTM B-172	Standard Specification for Rope Lay Stranded Copper Conductors Having Bunch-Stranded Members for electrical Conductors.
ASTM B298	Standard Specification for Silver Coated Soft or Annealed copper Wires.

ASTM B355	Standard Specification for Nickel Coated Soft or Annealed Copper Wires.
ASTM D4566	Standard Test Methods for Electrical Properties of Insulation and Jackets for Telecommunications Wire and Cable
CSA C22.2 no.0.3-92	Test Methods for Electrical Wires and Cables
ICEA S-66-524	Cross-Linked Thermosetting Polyethylene Insulated Wire and Cable for the Transmission and Distribution of Electrical Energy
ICEA T-22-294	Test Procedures for Extended Time Testing for Wire and Cable Insulation for Service in Wet Locations
ICEA T-28-562	Hot Creep
MIL-C-5015	Connector Specification
MIL-C-13777	Cables, Special Purpose, Electrical
MIL-C-24643	General Specification for Cables and Cords, Electrical, Low Smoke, for Shipboard Use
MIL-F-13927A	Electrical, Fungus Resistance Tests
UL 1581.	Reference Standard for Electrical Wires, Cables and Flexible Cords
MIL-STD-1344A	Test Methods for Electrical Connectors
MIL-STD-202F	Sand and Dust.
NEMA 4	Plugs, Receptacles and Cable Connectors
AAR S-4006	Performance Tests for Air Brake End Hose Supports
AAR S-471-92	Brake Pipe Restriction Test

2.2 Temperature Tolerances

All test temperatures stated in this document have a $\pm 2^{\circ}C$ tolerance.

3.0 GENERAL SERVICE INTER-CAR CABLE

3.1 General Characteristics

The cable shall consist of two #8AWG conductors and a shield. The conductors must have a minimum of two twists per foot. The cable shall be rated to 600V and a have a characteristic impedance of 50 Ohms ±10%. The operating temperature range is -45°C to 65°C. The overall outside diameter must be 0.700 inch minimum to 0.750 inch maximum. The dimensional tolerance for any given cable outside diameter is ±0.025 inches.

3.2 Conductors

3.2.1

Conductors shall be #8AWG and consist of annealed tinned copper per ASTM B-33 and shall have rope stranding sufficient to meet flexibility requirements.

3.2.2

The cross sectional area of the conductors shall not be less than 98% of the cross sectional area specified. Resistance values shall be in accordance with ICEA S-66-524.

3.3 Insulation, General Requirements

3.3.1

The insulated wire and cable shall be suitable for electrically controlled freight brake systems for the railroad industry and all requirements and parameters specified herein must be met.

3.3.2

The insulation shall be tight fitting over the stranded conductors and be clean stripping without damage to strands.

3.3.3

The insulation shall be fungus resistant and shall be tested in accordance with Mil-F-13927A. After thirty days, the material must be fungus inert.

3.3.4

The insulation thickness at any point shall not be less than 90% of the nominal average wall thickness to meet the requirements of section 3.1.

3.3.5

The insulation shall have a continuous temperature rating of 90°C as determined by test temperatures used, and temperature related parameters established herein. This cable is not certified for use within locomotive engine rooms. If cable is routed through locomotive engine rooms, the cable insulation must be rated at 125°C.

3.4 Insulation, Properties and Tests

Unless otherwise stated, all testing in section 3.4 will be done on samples removed from completed cable.

3.4.1 Unaged Tensile and Elongation

When tested in accordance with ICEA S-66-524, the minimum values measured on insulation samples which have been removed from the conductor shall be as follows:

Tensile strength - 750 psi. Elongation - 200%

3.4.2 Aged Tensile and Elongation

When tested as above, insulation which has been aged in a circulating air oven for 168 hours at 121°C shall have the following minimum values:

Tensile strength - 75% of unaged value Elongation - 75% of unaged value

3.4.3 Dielectric Proof Test

Insulated conductors shall withstand test voltages as specified in ICEA S-66-524 for five minutes after a six hour immersion in water. The water shall be normal tap water (conductive), and at room temperature. The sample shall be wound in a coil with a diameter of 20 times the insulated diameter. The required test voltage shall be 6.0 KV AC (RMS) and 18 KV DC.

3.4.4 Impulse Dielectric or Spark Test

100% of all wire made to this specification shall withstand either the dielectric proof test (3.4.3) or a 100% impulse dielectric test of 18.0 KV.

3.4.5 Insulation Resistance in 25°C Water

The center 20 foot section of a 25 foot length of insulated conductor shall be immersed in normal tap water which is maintained at 25°C for 24 hours. Following this conditioning period, the sample shall pass the dielectric proof test (3.4.3), and the insulation resistance shall be measured per ICEA procedures. The minimum acceptable insulation resistance value shall be calculated using the insulation resistance constant value K at 10,000. Resistance is calculated as:

$$R = K * \log(OD/ID)$$

3.4.6 Long Term Insulation Resistance

A sample shall be immersed for 26 weeks in a water bath maintained at 90°C, and with 600 volts rms applied continuously. Insulation resistance measurements shall be taken weekly. The

minimum acceptable insulation resistance value shall not be less than ten megohms based on 1000 feet after the 26 week test.

3.4.7 Long Term Direct Current Service Test

Insulation shall be evaluated for suitability for service in wet locations using the test specimens and procedure described in ICEA T-22-294. The water temperature shall be maintained at 90°C with a continuous test voltage of 600 volts DC negative applied to the conductor. The test shall be conducted for a minimum of 16 weeks. The minimum acceptable measured dissipation factor (power factor) shall not exceed 0.05.

3.4.8 Cold Bend Test

The cold bend test shall be run per UL-1581, paragraph 580 except the conditioning temperatures shall be -45°C, the sample shall not be removed from the cooling chamber when performing the test, and the mandrel size, tension weights, and number of turns shall be as indicated below:

Mandrel Size - 5/8", Tension Weights - 10 pounds, Number of Turns - 6

The insulation shall not exhibit visible cracks, and after bending, must pass the dielectric proof test (3.4.3).

3.4.9 Cold Impact Test

The cold impact test shall be run per UL-1581, paragraph 590, or per CSA C22.2 No.0.3-92, except the conditioning and actual test temperature shall be -45°C.

3.4.10 Cold Shock (unwind) Test

A sample shall be prepared with a length not to exceed two feet. The mandrel, tension weights, and number of turns shall be as indicated below:

Mandrel Size - 5/8"

Tension Weights - 10 pounds

Number of Turns - 6

The assembly shall then be conditioned at -45°C, for a minimum of one hour. While still at -45°C, the sample shall be unwrapped within the cold box at a speed of 15 RPM. The insulation shall not exhibit visible cracks, and shall pass the dielectric proof test (2.4.3).

3.4.11 Insulation Shrinkage Test

A 24-inch sample of completed wire shall be cut flush and straight at both ends. The sample shall be placed in a loose coil and condition in a circulating air oven for 168 hours at 121°C. Following the conditioning period, the sample shall be removed from the oven and allowed to cool for at least one hour at room temperature. The sample shall then be wrapped around a 3/8" mandrel for six turns and insulation shrinkage at both ends shall be measured. The maximum allowable shrinkage shall be 1/8" on either end.

3.4.12 Aged Insulation Resistance

A 25-foot sample coil of finished insulated wire shall be conditioned in a circulating air oven for 168 hours at 121°C. Following the conditioning period, the sample shall be removed from the oven and allowed to cool at room temperature for at least one hour. The sample must pass the dielectric proof test (3.4.3), and shall pass the insulation resistance test in 25°C water test (3.4.5).

3.4.13 Aged Cold Shock Test

A sample of finished insulated wire shall be conditioned in a circulating air oven for 168 hours at 121°C. The sample shall then pass the cold shock (unwind) test (3.4.10).

3.4.14 Penetration Test

A sample of the insulated conductor, jig, and plunger/chisel, shall be conditioned for a minimum of one hour at 121°C. The plunger/chisel shall consist of a metal plunger having a sharp chisel knife edge, (approximately 0.001 inch radius or less), with a provision for adding

weight. The plunger/chisel shall be positioned in a suitable metal jig with a 750 gram total weight. The sample shall be placed under, and a right angle to, the plunger/chisel cutting edge. After preconditioning the weighted plunger shall be gently lowered into contact with the cable surface. A six volt buzzer circuit between the conductor and the plunger/chisel shall be used to indicate a test failure. The weighted plunger/chisel shall then be raised, the wire sample rotated 120^{O} in the radial plane, and the test repeated. The process shall be repeated a third time, again rotating the sample 120^{O} in the radial plane. The sample shall not indicate a short circuit in ten minutes or less in any of the three trials.

3.4.15 Crush Resistance Test

Finished samples of wire shall be placed between two flat steel plates, (2-1/4" x 2-1/4" x 1/4") with corners and edges rounded to 1/8" radius, mounted parallel and in a horizontal plane. The plates shall be closed at a rate of 0.2 inches per minute until the conductor is grounded to either of the steel plates as indicated by a low voltage (6 volts DC) buzzer circuit. The crush resistance shall be the average of ten trials, all conducted at room temperature. The insulated conductor shall exhibit a crush resistance of at least 2,500 pounds.

3.4.16 Hot Creep Test

Test according to ICEA T-28-562 at 175°C. At the conclusion of the test the samples shall have the following minimum values:

Max. Elongation - 100%

Set - 5%

3.5 Fillers

Cables shall include fillers as necessary to insure that the finished cable diameter is as specified in section 3.1. Fillers used must be non-wicking and compatible with other cable components.

3.6 Binder

Cables may include a binder over the cable core, under the overall jacket. Additional binders may be used as necessary dependent on cable construction and manufacturing techniques. Binders used must be compatible with other components.

3.7 Shield

The shield shall be designed to significantly reduce the effects of electromagnetic and radio frequency interference (EMI/RFI) by shielding the cable core with a tinned copper braided shield. To insure the shield can effectively reduce EMI/RFI, the minimum shield resistance shall be three ohms/1000 feet (10 milli-ohms per meter) at 25°C. Minimum shield coverage is 85%.

3.8 Shield Drain Wire

The cable shall incorporate a drain wire for the shield. The drain wire shall be a minimum wire size of #22 AWG.

3.9 Jacket

A heavy duty, flexible low temperature material such as polychloroprene shall be used and shall have reinforcing served thread(s) located at approximately the middle of the jacket wall, and shall meet the following requirements.

3.9.1 Unaged Tensile and Elongation

When tested in accordance with ICEA S-66-524, the minimum values measured on jacket samples which have been removed from the cable shall be as follows:

Tensile Strength - 1,850 psi

Elongation - 200%

Modulus at 200% - 850 psi

20% set, max

3.9.2 Aged Tensile and Elongation

When tested as above in 3.8.1, jacket which has been aged in a circulation air oven for 168 hours at 100°C shall retain the following minimum values:

Tensile Strength - 80% retention of unaged value

Elongation - 80% retention of unaged value

3.9.3 Oil Aged Tensile and Elongation

When tested as above in 3.8.1, jacket which has been aged in ASTM #2 oil or equivalent for 18 hours at 120°C shall retain the following minimum values:

Tensile Strength - 80% retention of unaged value

Elongation - 80% retention of unaged value

3.9.4 Low Temperature Brittleness

When samples of jacket are tested in accordance with Mil-C-13777, the minimum acceptable low temperature brittleness value shall be at -45°C.

3.9.5 Sunlight Exposure

Test according to UL 1581, section 2000, Sunlight Resistance. After 300 hours of exposure, the cable shall retain the following minimum values:

Tensile Strength - 85% retention of unaged value

Elongation - 85% retention of unaged value

3.10 Completed Cable

Unless otherwise stated, all tests in section 3.9 will be done on samples of completed cable.

3.10.1 Abrasion Resistance Test

Test according to Mil-C-24643 except test apparatus shall be set up to test between the overall shield and the abrasion tool. The sample shall be in contact with the wheel for a minimum of 90°. The weight used shall be two lbs. The minimum acceptable cycles is 500.

3.10.2 Cold Bend Test

The cold bend test shall be run according to section 3.4.8 except that the mandrel size shall be ten times the finished jacketed diameter.

3.10.3 Cold Impact Test

The cold impact test shall be run according to section 3.4.9.

3.10.4 Flex Test

Test a sample of completed cable according to MIL-C-13777. The bend test shall use a 5/8" diameter mandrel and a 50 pound weight. At the conclusion of the test subject the cable to an insulation resistance test (3.4.5).

3.10.5 Crush Test

Test according to section 3.4.15.

3.10.6 Cable Identification

The cable shall be marked throughout its length at regular intervals on the surface of the jacket or on a marker tape pulled in directly under the jacket with the following information:

AAR Specification Number

Manufacturers Name

2/C 8 AWG, 600 V

Unique Part Number

Quarter and Year of Manufacture

3.10.7 Final Electrical Testing

3.10.7.1 Dielectric Proof Test

Measure the dielectric withstand voltage from conductor to conductor and conductor to shield. The required test voltage shall be 6.0 KV AC (RMS) and 18 KV DC.

3.10.7.2 Insulation Resistance

Measure insulation resistance conductor to conductor and conductor to shield at 500 VDC. The minimum insulation resistance shall be R = K*log(OD/ID) where the insulation resistance constant K = 10,000..

3.10.7.3 Conductor Direct Current Resistance

Minimum Requirements per section 3.2.

3.10.7.4 Shield Resistance

Measured in accordance to section 2 of ICEA S-66-524. Minimum requirements per section 3.7.

3.10.7.5 Cable Characteristic Impedance

Test according to ASTM D4566, Method 2, Option 1, at 250 KHz.

4.0 GENERAL SERVICE UNDER CAR CABLE

This cable shall meet all requirements of section 3.0 with the following exceptions.

4.1

A metal conduit, flexible conduit, cable armor, or equivalent which can accommodate this cable may be used at the option of the end user.

5.0 HIGH TEMPERATURE UNDER CAR CABLE

This cable is intended to be thermally insulated. A cable which meets all of the requirements of section 3 but with insulation rated at higher than 90°C may be required to meet the individual requirements of the railroad or car owner depending on car design and thaw shed characteristics.

6.0 INTER-CAR CONNECTORS

6.1 Electrical Qualification Test Procedure

6.1.1 Insulation resistance test

Mated pair, 500 V, 1 minute hold time. 500 Megohms minimum resistance. Conduct test between conductors and between conductors and shield.

6.1.2 High Potential Test

Mated pair, 2200 VDC, 5 minute hold, with a maximum accepted leakage of 5 micro amperes.

6.1.3 Wet Mate Test

Immerse two connectors in water, take out of water and immediately mate while still wet with the connectors in a horizontal position. Perform insulation resistance test (6.1.1) or Hi-Pot test.

6.2 Environmental

6.2.1 Salt Spray

Subject two unmated connectors to a salt spray per MIL-STD-1344A, Method 1001.1 Test Condition A. Mate connectors and make a voltage drop test (7.2.2) and make the insulation resistance test (6.1.1).

6.2.2 Humidity/Temperature Test

Test a pair of mated connectors per MIL-STD-1344, Method 1002, Test Procedure Type III. Immediately after completion of the last test cycle, conduct a voltage drop test (7.2.2) and an insulation resistance test (6.1.1). Then remove the connectors from the test chamber, un-mate and let sit at ambient conditions. Within 1 to 2 hours after removing from the chamber, re-mate and repeat the voltage drop test (7.2.2) and the insulation resistance test (6.1.1).

7.0 CONNECTOR ASSEMBLIES

A connector assembly is defined as an intercar connector, cable, and carbody junction box connector as described in section 8.1. The assembly may or may not be integrated with an air hose coupling.

7.1 Strength Member

7.1.1

The strength member will be external to the cable. It must support the connector such that the lowest point of the connector is 4 to 5 inches above the top of rail with the car fully loaded. The strength member must bear the pull apart forces.

7.1.2

The strength member must be capable of sustaining 200% of the maximum pull apart force..

7.1.3

The forces exerted during any disconnection must not result in damage to the portion of the connector on the car body junction box or to the permanent wiring on the car, even in the event of complete lanyard failure.

7.2 Mechanical Qualification Test Procedures

7.2.1 Definitions

For purposes of this specification, the following definitions pertain:

7.2.1.1

Un-Mate - uncoupling the connectors manually without uncoupling the cars themselves.

7.2.1.2

Pull-apart - uncoupling the connectors by uncoupling the cars. Pull apart forces must be through the external strength member.

7.2.2 Voltage Drop Test

Mated pair, 20 amp current, made at 66°C, room temperature and at -45°C. Apply current and measure the voltage drop. The maximum allowable post-test voltage drop of the assembled pair is 100 millivolts from end sill connector to end sill connector.

7.2.3 Durability

Run a pair of connector assemblies through 1000 mate/pull-apart cycles. Measure voltage drop before test, and after cycle #1, 250, 500, 750 and 1000. Voltage drop must not exceed the criteria defined in 7.2.2. Perform a insulation resistance test (6.1.1) as a final test. The pull apart forces must be measured at cycle #250, 500, 750 and 1000. The pull-apart forces must meet the test criteria in section 7.2.5. The mate forces must never increase to the point that a normal human being has difficulty in coupling the connectors.

7.2.4

Connector assemblies must be capable of being coupled/uncoupled under current industry railcar couplers, i.e rotary dump, bottom shelf, angle cock and traveling hose carrier designs. Coupling/uncoupling must be performed with a metal support strap meeting appropriate sections of current AAR specification S-4006.

7.2.5 Pull-Apart Forces

Measure the pull-apart forces at room temperature, at -45°C and at 66°C. Rate of separation should be at least 2 fps (1.4 mph). Connector assemblies should be soaked at the high and low test temperatures for a sufficient time to ensure that the connector assemblies reach the required temperature. The pull-apart forces must be no less than 100 pounds, and no more than 400 pounds. The mate forces must never increase to the point that a normal human being has difficulty in coupling the connectors. It must never be necessary to use tools to couple connectors.

7.2.6 Thermal Shock

Cycle mated connectors between -45°C and 66°C for 5 cycles. Connectors must be soaked at -45°C in one temperature chamber, then immediately placed in a second temperature chamber

and soaked at 66°C. Connectors must be soaked at the high and low test temperatures for a sufficient time to ensure that the connectors reach the required temperature. One cycle is defined as raising the temperature of the connector, then lowering the temperature in the reverse order. Examine for physical damage, loose fasteners, etc. At the completion of the 5 cycles, after reaching room temperature, conduct an insulation resistance test (6.1.1), a wet mate test (6.1.2) and a pull apart test (7.2.5, at room temperature only)

7.2.7 Physical Shock

Measure the initial mate/unmate forces and voltage drop. Suspend a mated pair of connectors from a 12 foot long rope or cable so that the connection point of the connector assemblies just comes in contact with a concrete wall or steel beam. Pull the connectors out from the wall until the connection point is raised six feet, then release. The mated connector assemblies should impact while in a vertical position. The connectors must be impacted on the bottom and one side. A suggested test fixture is shown in Figure 1. Impact a total of eight times per axis. Conduct this test at room temperature, -45°C and at 66°C. For the tests at the temperature extremes, conduct the tests within one minute from removing the connectors from the temperature chamber. Connectors must be soaked at the high and low test temperatures for a sufficient time to ensure that the connectors reach the required temperature. The mate/unmate forces must meet the test criteria in section 7.2.5. Voltage drop must not exceed that defined in 7.2.2. Conduct an insulation resistance test (6.1.1). Repeat physical shock test with a single unmated connector.

7.2.8 Extreme Temperature Pull Apart

Pull a mated pair of connector assemblies apart. Rate of separation should be at least 2 fps (1.4 mph). Prepare the cable assemblies by cooling them in a temperature chamber at -45°C and coat with a minimum of ½ inch of ice. Measure the force required to separate the connectors. Repeat by recoupling the connector assemblies, putting them back in the temperature chamber and re-establishing the ½ inch thick ice coating. Repeat for a total of 25 uncouplings. Make an insulation resistance test (6.1.1), a pull apart test (7.2.5) at room temperature only and a voltage drop test (7.2.2) before the first test and after the 25th uncoupling. Repeat this test with a pair of connectors heated to 66°C for 30 minutes minimum between each of 25 uncouplings.

7.2.9 Frozen Connector Mate Test

Prepare a pair of cable assemblies by cooling them in a temperature chamber at -45°C. Remove them from the chamber and immediately couple the connectors together. The mate forces must never increase to the point that a normal human being has difficulty in coupling the

connectors. It must never be necessary to use tools to couple connectors. It is permissible to knock the two connectors together to remove any ice before mating the connectors.

7.3 Environmental

7.3.1 Fluid Resistance

Test connector samples according to method 1016 of MIL-STD-1344 (one sample per fluid). The test fluids will be diesel fuel, lubricating oil (fluid type d), Isopropyl alcohol (fluid type I) and sulfuric acid (0.5% concentration). The connectors must be tested unmated. Following the fluid immersion cycles, the connectors must be mated without being wiped off, then given the pull apart test at room temperature only (7.2.5), an insulation resistance test (6.1.1) and a voltage drop test (7.2.2).

7.3.2 Sunlight Exposure

Test according to section 3.9.5.

7.3.3 Sand/Dust Exposure

Mated connectors will be tested according to method 110 of MIL-STD-202. Following the sand immersion cycles, the connectors must be given the pull apart test at room temperature only (7.2.5), a wet mate test (6.1.2) and a voltage drop test (7.2.2).

7.4 Life Test

7.4.1 Pre-Test

Perform insulation resistance test (6.1.1) and voltage drop test (7.2.2).

7.4.2 Aging

Place a mated pair of connector assemblies at 2 x rated voltage in a temperature chamber. Age the mated pair at 107°C for 168 hours.

7.4.3 Post Test

Perform insulation resistance test (6.1.1), voltage drop test (7.2.2) and pull apart test (7.2.5) at room temperature only.

8.0 CAR BODY CONNECTIONS

8.1 Connectors

All connectors used between the end-of-car cable and carbody connection will meet the appropriate requirements of this specification. The connector shall be designed so that the plug on the end of cable shall form the "weak link" in the connection so that the receptacle portion, attached to the junction box or conduit extension (see 8.3.1), shall not be damaged if the cable is snagged by track debris. The assembly shall be designed to withstand a pull-apart force of no less than 400 pounds to a maximum of 600 pounds in any direction.

8.2 Junction Box

The assembled junction box or enclosure at the end sill of the car and at the split to the CCD shall be sealed and meet the requirements NEMA 4. The junction box removable covers shall be secured with captive screws/fasteners to prevent loss of these items during inspection and repairs.

8.3 Car body Connector Mounting Envelope

The car body connection must be within a 15 inch radius sphere centered on the angle cock to hose connection

8.3.1

An alternate to the junction box will be a connector built into the end of the cable conduit. The end of the conduit must be solidly supported at the end of the car within 12 inches of the car body connector.

8.4.1 Cable Length

The length of the entire connector assembly must be 40 ±1 inches for conventional cars and 51 ±1 inches for rotary dump cars.

8.4.2

Cars with sliding center sills or end of car trolley arrangements will require an intermediate cable between the car body connection of the connector assembly and the car body itself. All wiring connections on the intermediate cable will use ring terminals.

8.5 Carbody Wiring Connections

8.5.1 Connection Types

All wiring connections on the car itself, for example from the main cable to the CCD, will use low resistance ring terminals and crimped connections. The ring terminals shall be bolted to suitably sized terminal posts with locknuts and plain washers or plain nuts with shake-proof washers, capable of withstanding a vibration level of ± 5g over a frequency range 20 - 80 Hz.

8.5.2 Connection Resistance

The electrical resistance of bolted and crimped connections shall not exceed 10 milli-ohms.

8.5.3 Cable Shield Grounding

The cable shield shall be grounded to the car body at the junction box containing the live connections to the CCD, using ring terminals crimped to the drain wire bolted to terminal posts as specified in 8.5.1.

9.0 CRIMP STRENGTH

9.1 Crimp Tensile Pull Test

The sample contact shall be attached to the specified #8 AWG wire and placed in a standard tensile-testing machine. Sufficient force shall be applied to pull the wire out of the sample contact or break the wire or the sample. The travel speed of the head shall be one inch per minute. The clamping surfaces may be serrated to provide sufficient clamping force. During the pull test, the sample contact shall not break or separate from the wire before the minimum tensile strength of 150 pounds is reached.

10.0 APPROVAL PROCEDURE

10.1

The manufacturer will apply in writing to the Director, Technical Committees-Quality Assurance, Mechanical Division, Association of American Railroads, 50 F Street NW, Washington, DC, 20001, to initiate the approval process. This application for approval will include a description of the product and its intended use.

10.2

The manufacturer will, at no expense to the AAR, provide a sample of each cable and/or connector to each member of the Brake Systems Subcommittee.

10.3

The manufacturer will supply at least 500 feet of production cable, or 50 production connector assemblies, from which an AAR representative will select the necessary test samples.

10.4

The manufacturer will provide test data and certify that the cable and/or connector meets all requirements of this specification. Testing must be performed or witnessed by the AAR Research

and Test Department, or be conducted by a certified outside laboratory. The AAR may, at their discretion, require further testing at any time to ensure continued compliance.

10.5

After the Brake Systems Sub-committee examination of the cable and supporting information, the Sub-committee will notify the manufacturer or supplier as to whether the product has been given a conditional approval or has been disapproved.

A4 AAR SPECIFICATION S-4220

Specification S-4220

PERFORMANCE SPECIFICATION FOR ECP BRAKE DC POWER SUPPLY

Adopted: May, 1997

1.0 PURPOSE

The supply of electrical power to the Electronically Controlled Pneumatic (ECP) brake controllers and the other electronic components on the freight car is vital to the safe and reliable operation of the system. The power on each car is maintained through a rechargeable battery system, at a nominal voltage of 12 VDC. The purpose of the ECP power supply is to provide the battery charging supply from the locomotive(s) in the consist to each car, through the hardwire trainline, sharing the same conductors with the communication signals (power line overlay mode). It is therefore essential that the quality of the electrical power supplied to the line be sufficiently well controlled so as not interfere with the communications. The basic requirement of the ECP power supply is that it converts a nominal 74 VDC (locomotive battery) supply and delivers a 230 VDC supply to the trainline at a power level of 2500 watts. The converter may also be required to provide an optional auxiliary 24 VDC supply, rated at 150 watt, to power the displays, the computer and other auxiliary loads within the head end brake controller.

2.0 ELECTRICAL PERFORMANCE

2.1 Input Voltage

The converter input is nominally 74 VDC with an operating range from 40 VDC to 100 VDC, with the following provisions:

2.1.1 Input Isolation

Input and output conductors shall be isolated from the chassis and from one another to withstand 2.5 KV rms.

2.1.2 Input Ripple

The converter shall provide the specified output in the presence of the following input ripple voltages with the input at nominal voltage: 18 Vp-p from DC to 6 KHZ, reducing linearly to 4 Vp-p at 50 KHz, remaining at 4 Vp-p to 250 MHZ, thereafter reducing linearly to 0.1 Vp-p at 400 MHZ.

2.1.3 Input Protection

The converter shall not be damaged by input voltages in the range from 25 VDC to 135 VDC, or by input spikes of ±2 KV, having a duration of 50 microseconds, containing 0.05 Joules of energy and occurring at the rate of 10 spikes per second.

2.1.4 Inrush Current

When commanded "ON", the converter in-rush current shall not exceed 200 amperes.

2.2 Output Voltage

2.2.1 Voltage Range

The converter primary load output voltage is nominally 230 VDC. Under all line and load conditions, the output voltage shall remain in the range from 212 VDC to 248 VDC.

2.2.2 Voltage Ripple

The maximum voltage ripple shall not exceed 100 mV p-p.

2.2.3 Voltage Regulation

The output voltage shall not vary by more than ±8% from nominal for combined no load to full load and rated input voltage change.

2.3 Output Impedance

The power supply differential mode output impedance shall not be less than 2 k ohms in the frequency range 100 KHz to 450 Khz.

2.4 Output Current

The output current shall nominally be in the range from 0.1 A minimum to 10.9 A maximum. The load will be capacitive from DC to 4 KHz and inductive at all higher frequencies.

2.5 Output Load Transients

The output shall be capable of withstanding a load inrush current of 130 amperes decaying logarithmically to 10.9 A in 15 milliseconds, with recurring 1 ampere peaks at a 100 KHz rate.

2.6 Output Protection

2.6.1 Current Limit

The output shall current limit at 15 amperes nominal and will return to normal operation when the overload is removed.

2.6.2 Overvoltage

The output overvoltage shall be set at 250 VDC ± 0.5%. If this voltage is exceeded, the converter will latch "OFF" requiring the input power to be turned "OFF" to reset.

2.6.3 Line Voltage Polarity

The output control of the power supply shall incorporate an automated means to detect the presence and polarity of an existing supply on the trainline and to prevent the closure of the output breaker in the event of a polarity mismatch. In order to minimize the risk of malfunction it is recommended that a 3 sec measurement period be used to determine the line voltage polarity.

If no existing supply is detected then the power supply is free to apply a voltage at its default polarity.

2.6.4 Reverse Polarity Protection

Since the polarity of the trainline supply voltage cannot be predefined, adequate protection shall be provided to ensure that the power supply (including any output filter circuits) not be damaged by reverse polarity energization from the trainline.

2.7 Output On/Off Control

The output On/Off control shall be interlocked with the trainline communications system so that the 230 VDC supply can only applied to the trainline when the lead locomotive head-end unit (HEU) and end-of-train (EOT) beacon messages are being received and the power supply has been "enabled" (armed) by the HEU. **Please note that these requirements are intended to permit the control of any power supply in the train from the lead locomotive and to facilitate the use of multiple power supplies for very long trains.** The power supply control function may be provided by one of two methods.

2.7.1 External Control

The output voltage at the power supply will be turned "ON" and "OFF" in response to the closing (ON) or opening (OFF) of a set of external contacts, located in a separate control box. These contacts will be rated for a maximum current of 50 mADC.

A separate control box will be provided with the capability of providing the 50 mADC current to the control terminals of the power supply in response to control messages from the HEU and the presence of the HEU/EOT beacons. As a minimum, it is expected that the control box would include an Echelon PLT10A transceiver or equivalant with a neuron based microprocessor or equivalent to provide the control intelligence.

2.7.2 Integrated Control

The output voltage at the power supply will be turned "ON" and "OFF" in response to the HEU control and beacon messages by means of a Echelon PLT10A compliant device integrated directly into the power supply. The features of the integrated control system shall be compatible with those specified for the external control, described in section 2.7.1.

2.8 Auxiliary Output

An **optional** auxiliary output may be required, with the following characteristics:

2.8.1 Output Voltage

The output voltage shall be 24 VDC ± 1%. The maximum voltage ripple shall not exceed ± 5 mV p-p.

2.8.2 Output Current

The rated output current shall be 0 to 6.0 A

2.8.3 Output Control/Protection

If provided, the control of the auxiliary supply shall be completely independent of the primary load supply. The auxiliary output shall be protected by a breaker or "slow blow" type fuse, rated at 15 A.

3.0 ELECTROMAGNETIC COMPATIBILITY

3.1 Radiated Emissions

Radiated emissions must not exceed 30,000 μV/m (micro-volts per meter) below 200 KHz decreasing to 100 μV/m at 27 MHZ. Specially guarded bands are:

30 μV/m from 27.2 MHZ to 27.3 MHZ

30 μV/m from 158 MHZ to 165 MHZ

70 μV/m from 450 MHZ to 460 MHZ

3.2 Output Conducted Emissions

Output conducted emissions shall generally meet the requirements of FCC Section 15.107. Specifically, the conducted emissions may not exceed 100 dbμV at 20 KHz, decreasing to 50 dbμV at 130 KHz and continuing to 450 KHz, with 12 db/decade rise above 450 KHz.

3.3 Input Conducted Emissions

Input conducted emissions may not exceed 0.3 V p-p from 30 Hz to 50 KHz and 10 mV p-p from 50 KHz to 400 MHZ.

4.0 ENVIRONMENTAL CONDITIONS

The converter will operate under the following conditions or natural combinations of conditions:

4.1 Operating Temperature

The converter will operate within the temperature range from - 45 °C to + 70°C.

4.2 Storage Temperature

The converter may be stored within the temperature range from - 50°C to + 85°C.

4.3 Vibration

The converter will survive and operate in an environment where it will experience the following vibration input:

frequency range 5 to10 Hz 0.3 in amplitude sine wave

frequency range 10 to 300 Hz a level of 3g in any axis

4.4 Shock

The converter will survive and operate in an environment where it will experience shock at a level of 3g for 11 milliseconds half sine wave in any axis.

4.5 Rain/moisture Intrusion

The converter enclosure shall be sealed so that it is capable of operating in a water saturated environment, such as the cavity below the locomotive cab floor or inside the nose compartment of the locomotive, where the door may have been left open . Direct water spray testing to NEMA 250-1991 M6.7.1 or equivalent will be accepted as evidence of compliance with this requirement.

4.6 Mounting Orientation

The converter shall be made available in models for rack, bulkhead or deckplate mountings.

4.7 Airflow

The converter shall be cooled by natural convection and shall not depend on ambient airflow for cooling. Stirring fans may be used internally to circulate the air over the heatsinks and break up any hot spots, provided that adequate protection is provided against malfunction of the power supply due to their failure.

5.0 MECHANICAL AND INSTALLATION

5.1 Dimensions

The converter dimensions will not exceed 19" wide by 15 " deep by 10.5" high.

5.2 Weight

The converter weight will not exceed 50 pounds.

5.3 Electrical Connections

The input and output connections shall be made using ring terminals bolted to terminal strips with locknuts or plain nuts with shake-proof washers, capable of withstanding a vibration level of ± 3g over a frequency range of 20 - 80 Hz. A protective cover must be provided for the electrical connections.

5.4 Adjustment

The converter shall require no external adjustments

5.5 Warmup Time

The converter shall provide full rated performance within one second after the ON contact closure is made.

Specification S-4230

INTRA-TRAIN COMMUNICATION SPECIFICATION

Adopted: May, 1997

1.0 INTRODUCTION

This specification was prepared by the Association of American Railroads in cooperation with their member railroads and the supply industry. The detailed contents were developed through an open forum process of public meetings. The purpose of this specification is to define the requirements for an intra-train communications system for freight equipment in revenue interchange service. The specification is intended to facilitate interoperability between freight cars and locomotives, without limiting the proprietary design approaches used by individual suppliers.

The intended use of the intra-train communications system is control of electronically controlled pneumatic (ECP) brakes and remote multiple units (distributed locomotives), and the continuous monitoring and safety reporting of various components on freight cars and locomotives.

2.0 SCOPE

This document sets forth the requirements for an intra-train communication system. This specification outlines the basic communications hardware, system protocol, and message and performance requirements trainline communication network. The specification designates off-the-shelf communications technology, for the purpose of reducing both the cost and time required to bring the benefits of electrically controlled brakes, distributed motive power, and safety/health monitoring to the railroad industry.

The inherent principle behind this specification is to define only those necessary interfaces between vehicles within the train, in order to maintain system-wide interchange of cars, while defining performance levels for sub-system components. The performance requirements are intended to encourage high performance, low cost and maintenance, and high reliability equipment designs. Equipment suppliers are free to accomplish these requirements by means of unique designs and technology that they consider to be cost

effective and appropriate. Suppliers and railroads producing and purchasing systems in accordance with this specification are responsible for ensuring that all regulatory and safety requirements are met.

3.0 ECP BRAKE SYSTEM REQUIREMENTS

3.1 General

3.1.1 Protocol

To promote the highest reasonable level of interoperability, all nodes using the electric trainline communication media must fully implement the LonTalk protocol in the manner prescribed in this document.

3.1.2 Transceiver Compatibility

In order to control conducted noise on the electric trainline communication media, all transceivers accessing this media must be compatible with the Echelon model PLT-10 transceiver.

3.1.3 Variable Type Convention

The following variable type convention is used in this document:

`[signed] long int`	16 bit quantity
`unsigned long int`	16 bit quantity
`signed char`	8 bit quantity
`[unsigned] char`	8 bit quantity
`[signed] [short] int`	8 bit quantity
`unsigned [short] int`	8 bit quantity
`enmun (int type)`	8 bit quantity

3.14 Device Documentation

3.1.4.1 Program Identification

This ID is used to identify the type of device. It is a 8 byte value. This ID is specified by the following compiler directive:

```
#pragma set_std_prog_id f:mmm:cc:cc:ss:nn:vv:vv
```

where:

f = format type. This is to be set to fm = 8.

mmm = Manufacturer ID. 12 bits. Additional manufacturer ID numbers will be assigned as required. The current manufacturer ID numbers are:

Value	Manufacturer
1	NYAB
2	TSM
3	WABCO
4	Zeftron
5	Honeywell
6	GE/Harris
7	Graham White
8	MA/COM

cc = device class. Additional device classes will be assigned as required. The current device classes are:

Value	Device Type
1	CCD
2	DPM
3	EOT
4	HEU
5	Power Supply
6	Event Recorder

ss = device subclass.

nn = model number.

vv = software version

3.1.4.2 Vehicle Identification

The reporting mark and other vehicle data is made available to the network as the vehicle information network variable. The vehicle information network variable is a `config` class network variable. The contents of the vehicle information network variable is stored in EEPROM and can only be changed by another node on the network (i.e. a network manager).

The vehicle identification should be provided to the HEU by every vehicle in the train through the use of the `vehicle_ID` network variable.

The `vehicle_ID` network variable uses the following data structure:

```
typedef struct vehicle_id
      {
      char            report_mark[11];
      char            aar_type[4];
      unsigned        length;
      } vehicle_id;
```

field descriptions for **`vehicle_id`**:

- **`report_mark`** contains the car reporting mark.
- **`aar_type`** is the AAR car type code.
- **`length`** is the length over pulling faces (stretched) of the vehicle in feet with a one (1) foot resolution.

3.1.4.3 Network Variable Self Documentation

Network variables should be documented in a common manner. The network variable self documentation strings are given with the network variable table data.

3.1.4.4 Allowed Device Types

In order to effectively manage the message bandwidth and protect the signal integrity of the trainline communication network, only devices described within this document are allowed access to transmit messages on the trainline communication network while the train is in operation. Furthermore, these devices must fully comply with the guidelines governing message frequency and use.

The allowed device types are:

- Head End Unit (HEU),
- End of Train Device (EOT),
- Car Control Device (CCD),
- Power Supply Controller (PSC),
- Distributed Power Module (DPM),
- any passive (non transmitting) device, such as an event recorder, is allowed.

3.2 The Head End Unit (HEU)

No more than one HEU may be present in a locomotive, and only one HEU may be operating as a brake system controller in a train.

3.2.1 Function

3.2.1.1 Brake System Control

The Head End Unit, or HEU, is the control unit for the ECP Brake System.

3.2.1.2 User Interface

The HEU may connect to the user interface either directly or through a Locomotive System Integration (LSI) interface, if the locomotive is so equipped.

3.2.1.3 Locomotive Systems Integration (LSI) Interface

In order to maintain information/communication integration, the HEU will contain a LSI communication interface for those locomotives so equipped.

3.2.1.4 ECP Brake System Network Management

The HEU is responsible for the following basic network management services:

- Node/vehicle detection,
- Logical address assignment,
- Train database management,
- Event/exception logging,
- Network supervisory functions.

In order to promote interoperability of equipment, network management services are to be performed using LonWorks® network management messages and services.

3.2.1.4.1 ECP Brake Subnet / Node Address Assignment

The following guidelines should be used in assigning subnet / node addresses to self installing devices in the ECP Brake system:

- Subnets 1 through 9 are reserved for ECP brakes.
- The active (master) HEU is SUBNET 1 and NODE 1.

- A passive HEU is any address except SUBNET 1 and NODE 1 or SUBNET 1 and NODE 2.

- The EOT is SUBNET 1 and NODE 2.

3.2.1.5 Multiple HEU Handling

The HEU is configurable as either an active (master) unit or as a passive (slave) unit. Only the active HEU may send command messages. In order to prevent the occurrence of multiple active HEUs in the network, a HEU should default to a passive mode. Only an appropriate input from the train operator will cause an HEU to become active. An HEU must "listen" for the existence of another HEU for three seconds before becoming active. An HEU must remain inactive if the presence of an active HEU is detected.

If a locomotive containing an active HEU is added to a train already containing an active HEU then all active HEUs must warn the operator of the conflict. Also, emergency brake application must be made, and all active HEUs must become passive.

3.2.2 HEU Output Messages

3.2.2.1 The HEU Beacon

The purpose of the HEU beacon is to convey the current brake command to all nodes connected to the trainline communication network. The HEU beacon also serves as an indication of trainline continuity. The HEU Beacon is a **priority** message. This message is to be broadcast to all nodes in the network with no acknowledgments.

One CCD is polled each second by the HEU. The subnet & node address of the CCD being polled is contained within the HEU beacon. When polled the CCD should respond by transmitting a CCD Status message to the HEU. If a CCD fails to respond to two polls it is logged as inoperative by the HEU.

3.2.2.1.1 Contents of the HEU Beacon

The HEU data structure is used for the HEU beacon message.

```
typedef struct heu_data_struct
     {
      unsigned       mode;
      unsigned       brake_apply_percent;
      unsigned       subnet;
      unsigned       node;
      } heu_data_struct;
```

Field Descriptions:

- **mode** is the operating mode for the entire brake system. Performance definitions of these modes is provided in the ECP Brake Performance Specification, S*** section * of the AAR Manual of Standards and Recommended Practices. The following table provides the defined values for the mode field:

Mode

Value	Definition
0	Run (normal)
1	Road Switch Mode (CCD perform normally)
2	Initial Terminal Test
3	Yard Switch Mode (CCD go to release when requested)
4	Initialization Mode (clear exceptions)
5	Special Purpose Mode
6	Software Download Mode
255	ECP Overlay Cut Out

- **`brake_apply_percent`** is the desired brake application level for the CCDs
- **`subnet`** is the subnet of the next CCD to respond with a status message.
- **`node`** is the node number of the next CCD to respond with a status message.
-

3.2.2.1.2 Frequency of the HEU Beacon

The HEU beacon is broadcast to all nodes in the train once per second. An HEU beacon containing an emergency brake command will be issued immediately upon operator request.

3.2.2.2 Vehicle Configuration

The vehicle configure message is used to update data stored on an individual CCD which affects the performance of the vehicles braking system. A default value for each parameter must be stored on the CCD for use if a different value is not specified from the HEU. This message should be addressed to an individual CCD and is to be acknowledged.

3.2.2.2.1 Contents of the Vehicle Configuration Message

The vehicle configuration message contains the following data structure:

```
typedef struct vehicle_config_data
    {
    unsigned        config_switch;
    unsigned long   net_braking_ratio;
    };
```

Field description for **`vehicle_config_data`**:

- **`config_switch`** is a bitfield containing switchable data for setting up CCD. `config_switch` uses the following bitfield:

  config_switch

bit	Definition	Default
A (LSB)	0 = Loaded, 1 = Empty	0 = Loaded. This is overridden by on board load sensor
B	spare	-
C	spare	-
D	spare	-
E	spare	-
F	spare	-
G	spare	-
H	spare	-

- **net_braking_ratio** is the target net braking ratio for the vehicle in one tenth (0.1) of a percent.

3.2.2.2.2 Frequency of the Vehicle Configuration Message

The vehicle configuration message is sent on a as needed basis.

3.2.2.3 Train Configuration

The train configure message is used to update data stored on an all CCDs in the train which affects the performance of the vehicles braking system. A default value for each parameter must be stored on the CCD for use if a different value is not specified from the HEU. This is a broadcast message and should only be used with unit trains which are uniformly loaded. This is a broadcast message and should be repeated three (3) times with no acknowledgments.

If a vehicle cannot comply with the requested train braking ratio, then it should use the closest possible net braking ratio.

3.2.2.3.1 Contents of the Train Configuration Message

The train configuration message contains the following data structure:

```
typedef struct train_config_data
     {
     unsigned        config_switch;
     unsigned long   train_braking_ratio;
     unsigned        feed_valve_setting;
     };
```

Field description for **train_config_data**:

- **config_switch** is a bitfield containing switchable data for setting up CCD. config_switch uses the following bitfield:

config_switch

bit	Definition	Default
A (LSB)	0 = Loaded, 1 = Empty	0 = Loaded. This is overridden by on board load sensor
B	spare	-
C	spare	-
D	spare	-
E	spare	-
F	spare	-
G	spare	-
H	spare	-

- **`train_braking_ratio`** is the target net braking ratio for the train in one tenth (0.1) of a percent. If this is set to zero (0), then each vehicle should use its default net braking ratio.

- **`feed_valve_setting`** is the brake pipe pressure for the train in PSIG. This has a resolution of one (1) PSI.

3.2.2.3.2 Frequency of the Train Configuration Message

The vehicle configuration message is sent on a as needed basis.

3.2.2.4 Time Synchronization

In order to promote coherent event tracking, the time synchronization message is used to set the internal clocks of all nodes in the network to approximately the same time. The time should be set to Eastern Standard Time (EST). This message is broadcast to all nodes in the network and should be repeated three (3) times with no acknowledgments.

3.2.2.4.1 Contents of the Time Synchronization message

The synchronization message contains the time stamp standard network variable (SNVT). The description of this SNVT is provided in appendix B.

3.2.2.4.2 Frequency of the Time Synchronization message

The time synchronization message is broadcast to all nodes in the train on an as needed basis. Primarily when the train network is setup and when vehicles are added en route.

3.2.2.5 Change CCD Status

The change CCD Status message is used to change the operating status or mode of an individual CCD. This message is addressed to an individual CCD and should be acknowledged.

3.2.2.5.1 Contents of the Change CCD Status message

The change CCD Status message contains the following data structure.

```
typedef struct change_status_struct
     {
     unsigned  status;
     } change_status_struct;
```

Field Descriptions:

- **status** is the current status of the CCD.

status

bit	Definition	Default
A (LSB)	0 = cut out, 1 = cut in	1 = cut in
B	spare	-
C	spare	-
D	spare	-
E	spare	-
F	spare	-
G	spare	-
H	spare	-

3.2.2.5.2 Frequency of the Change CCD Status message

The Change CCD Status message is sent on an as needed basis.

3.2.2.6 Exception Update Request

The exception update request is used when an unknown exception message is received by the HEU. This message is addressed to the node which generated the unknown exception message. This message is acknowledged with an exception update from the target node.

3.2.2.6.1 Contents of the Exception Update Request

The data structure for the request for an exception code update is:

```
typedef struct exception_update_rq_struct
    {
    unsigned  long code;
    } exception_update_rq_struct;
```

Field Description:

- code is the unknown exception code.

3.2.2.6.2 Frequency of the Exception Update Request

The exception update request message is sent on an as needed basis.

3.2.2.7 End of Train (EOT) Command

The EOT command is used to request the end of train device to perform a special function. The EOT command is addressed to the EOT and should be acknowledged.

3.2.2.7.1 Contents of the EOT Command

The EOT Command structure is used for the EOT Command message.

```
typedef struct eot_command_struct
    {
     unsigned  command;
    } eot_command_struct;
```

Field Description:

- **command** is the current command sent to EOT. **Command** is a bit field which uses the following definition:

command

bit	Definition
A (LSB)	spare
B	0 = marker off, 1 = marker on
C	0 = blue flag off, 1 = blue flag on
D	spare
E	spare
F	spare
G	spare
H	spare

3.2.2.7.2 Frequency of the EOT Command

The EOT command is sent on an as needed basis.

3.2.2.8 Power Supply Enable

3.2.2.8.1 Contents of the Power Supply Enable Message

The power supply enable message uses the SNVT State. The enable/disable bit of SNVT State is used to indicate whether a power supply controller (PSC) will activate a given power supply. This message is sent to each PSC in the train individually.

3.2.2.8.2 Frequency of the Power Supply Enable Message

The power supply enable message is transmitted during the initial setup of a locomotive containing a PSC. Also, this message may be sent on an as needed basis.

3.2.2.9 Power Switch

3.2.2.9.1 Contents of Power Supply Switch Message

The power supply switch message uses the SNVT State. The on/off bit of SNVT State is used to command the PSCs to turn on all enabled power supplies. In order to have all power supplies activate at approximately the same time, this message must be broadcast. Note that power will not be supplied to the electric trainline until both the power supply switch message and the EOT Beacon message are received by the PSC.

3.2.2.9.2 Frequency of Power Supply Switch

The Power Supply Switch message is transmitted on an as needed basis.

3.2.3 Input Messages for the Head End Unit (HEU)

3.2.3.1 End of Train (EOT) Beacon

The HEU expects to receive the EOT beacon once every second. If the HEU fails to receive three (3) consecutive EOT beacons, the train operator is alerted, and the next HEU beacon contains an emergency brake command.

3.2.3.2 CCD Status

The CCD status is received from one CCD each second as a response to the HEU beacon. If an active CCD fails to respond when polled, the HEU should poll the same CCD again with the next HEU beacon. If the CCD still fails to respond to two (2) retries (a total of three polls), then the CCD should be logged as unable to communicate. When a CCD is logged as unable to communicate it is only polled a single time with no retries by the HEU.

3.2.3.3 Exception Message

When the HEU receives an Exception message it must log the exception and the vehicle ID of the node which transmitted the exception and the time of the exception. The train operator should be alerted to the exception is necessary.

3.2.3.4 Broadcast Exception

When the HEU receives a broadcast Exception message it must log the exception and the vehicle ID of the node which transmitted the exception and the time of the exception. The train operator should be alerted to the exception is necessary.

3.2.3.5 Exception Update

When an exception update is received it should be stored by the HEU for future reference.

3.2.3.6 Vehicle ID

The Vehicle ID should be stored in a database within the HEU with the corresponding subnet and node address for the vehicle.

3.2.3.7 Vehicle Data

This message provides fixed information about a vehicle.

3.2.4 Network Image Definition for the Head End Unit (HEU)

To facilitate interoperability of nodes within the train network, the HEU should implement the following network image.

Domain Table

index	id[DOMAIN_ID_LEN]	subnet	node	len	key
0	-	set @ install	set @ install	0	0

- The HEU is only a member of one domain.
- Only one domain exists in the Train Control Network therefore zero length domain length is used.
- The lead HEU is always subnet 1 and node 1.
- Authenticated services are not used.

HEU Addr Table

Index	type	grp type	size	domain	backlog	node	member	rpt_timer	retry	rcv_timer	tx_timer	group	subnet
0	3	0	0	0	1	n/a	0	1 (24 mS)	0	3 (384 ms)	9 (384 ms)	0	0
1 (s/n to EOT)	1	0	n/a	0	n/a	2	n/a	8 (256 mS)	3	3 (384 ms)	9 (384 ms)	n/a	1

- Messages from the HEU which use address index zero (0) are domain wide broadcast.
- Backlog is set to one (1) since no acknowledgments are generated.

HEU Network Variable Configuration Table

NV Name	SD String	Priority	Direction	Hi Sel	Low Sel	Turn Around	Service	Addr Index
HEU Beacon Out	"@heul01.heu_beacon_out"	yes	out	0x00	0x00	no	2 (UNACKD)	0 (b.cast)
EOT Beacon In	"@heul02.eot_beacon_in	yes	in	0x00	0x01	no	-	15
Status In	"@heul03.status_in"	no	in	0x00	0x02	no	-	15
Exception In	"@heul04.except_in"	no	in	0x00	0x03	no	-	15
B.Cast Except In	"@heul05.bcast_except_in"	no	in	0x00	0x04	no	-	15
Vehicle ID Out	"@heul06.vehicle_info_out"	no	out	0x3F	0xF9	no	0 (ACKD)	15
Vehicle ID In	"@heul07.vehicle_info_in"	no	in	0x00	0x05	no	-	15
Vehicle Config. Out	"@heul08.vehicle_config_out"	no	out	0x3F	0xF8	no	0 (ACKD)	15
Time Synch Out	"@heul09.time_synch_out"	no	out	0x00	0x0A	no	2 (UNACKD)	0 (b.cast)
Change CCD Status	"@heul10.change_ccd_out"	no	out	0x3F	0xF6	no	0 (ACKD)	15
Exception Update	"@heul11.except_update_in"	no	in	0x00	0x06	no	-	15
Vehicle Data In	"@heul12.vehicle_info_in"	no	in	0x00	0x07	no	-	15
EOT Command	"@heul13.eot_command_out"	no	out	0x00	0x08	no	0 (ACKD)	1 (s/n to EOT)
Excpt. Update RQ.	"@heul14.excpt_updt_rq_out"	no	out	0x3F	0xF2	no	2 (UNACKD)	15
Train Config Out	"@heul15.train_config_out"	no	out	0x00	0x09	no	2 (UNACKD)	15
Power Supply Enable	"@heul16.psc_enable_out"	no	out	0x3F	0xF1	no	0 (ACKD)	15
Power Switch	"@heul17.psc_switch_out"	no	out	0x3F	0xF0	no	0 (ACKD)	15

- Bound ECP brake network variables use selector range 0x0000 to 0x0FFF.
- Unbound network variables use selector range 0x3000 to 0x3FFF.

3.3 The Car Control Device (CCD)

3.3.1 Function of the CCD

The function of the CCD to regulate the brake cylinder pressure of a vehicle. The CCD should perform in accordance with the ECP Brake Performance Specification, S*** section * of the AAR Manual of Standards and Recommended Practices. No more than one CCD should active on a single car or, in the case of multi-platform articulated cars, no more than one CCD per platform.

If a Standard Car Network interface is provided within the CCD it must comply with section 4 of this document.

3.3.2 CCD Output Messages

3.3.2.1 CCD Status

When the logical address of a CCD is designated within the contents of the HEU beacon then that CCD must return a CCD status message to the HEU. This message is unacknowledged.

3.3.2.1.1 Contents of CCD Status Message

The CCD Status Data structure is used by the CCD status message.

```
typedef struct status_data_struct
      {
     unsigned  status;
     unsigned  battery_volts;
     unsigned  brake_pipe_pressure;
     unsigned  supply_res_pressure;
     unsigned  percent_brake;
     };
```

Field Descriptions:

- **status** is the current status of the CCD.

status

bit	Definition	Default
A (LSB)	0 = cut out, 1 = cut in	1 = cut in
B	spare	-
C	spare	-

D	spare	-
E	spare	-
F	spare	-
G	spare	-
H	spare	-

- **battery_volts** is the voltage of the devices battery with a resolution of one tenth (0.1) volt.
- **brake_pipe_pressure** in PSIG with a resolution of one (1) PSI.
- **aux_res_pressure** in PSIG with a resolution of one (1) PSI.
- **percent_brake_cyl** is the current percent of braking effort of the CCD with a resolution of one (1) percent.

3.3.2.1.2 Frequency of CCD Status Message

The CCD status is sent to the HEU when requested in the brake command.

3.3.2.2 Exception Message

The exception message is used to transmit information to another node(s) within the network. Only conditions which need to be logged or acted upon should generate an exception message. Appendix A contains a list of defined exception codes, priorities for the exception, and what devices should receive the exception message. A unicast exception should be acknowledged, but a broadcast exception should not be acknowledged.

3.3.2.2.1 Contents of Exception Message

The exception code structure is used by the following messages:

- (CCD) Exception
- (CCD) Broadcast Exception

```
typedef struct exception_code_struct
     {
     char            ccd_id[11];
     unsigned  long  code;
     unsigned  long  data;
     int             priority;
     };
```

Field Descriptions:

- **ccd_id** is the ID of the device generating the exception (car reporting mark).
- **code** is the exception code. A list of defined codes is provided in appendix A
- **data** is additional data which may be required by the HEU.

- **priority** Indicates the severity of the exception, and the recommended action which should be taken.

Priority

Code	**Description**
0	exception clear
1	train must be stopped emergency rate
2	train must be stopped immediately at service rate
3	train must be stopped immediately at service rate if three or more like messages of this priority are received within 10 seconds.
4	reduced speed to next convenient point
5	maintenance required at next terminal
6	maintenance required at destination terminal
7	record and notify operator a CCD is cutout
8	record only
9	Event / No need to clear.

3.3.2.2.2 Frequency of Exception Message

Exception messages are transmitted on an as needed basis. Once an exception is transmitted from a node, it is not retransmitted unless the priority of the condition changes.

3.3.2.3 Exception Update

When an unknown exception code is sent to the HEU, the HEU may request an exception code update from the sending node. The response to the exception update request is the exception update message.

3.3.2.3.1 Contents of Exception Update

The data structure for the exception code update is:

```
typedef struct exception_update
    {
     unsigned long code;
     char                description[28];
     } exception update;
```

Field Descriptions:

- **code** is the exception code number.
- **description** is a string up to twenty-eight (28) characters in length. This contains a description of the code.

3.3.2.3.2 Frequency of Exception Update

The Exception update message is transmitted on an as needed basis.

3.3.3 Input Messages for the CCD

3.3.3.1 HEU Beacon

When the HEU beacon is received by a CCD, the CCD should set the target brake cylinder pressure accordingly. If the CCD's subnet and node address is contained in the HEU beacon, then the CCD should respond by sending a CCD status message to the HEU.

3.3.3.2 EOT Beacon

A CCD should respond to the absence or presence of the EOT Beacon in accordance with the Performance Requirement for Testing Electrically Controlled Pneumatic Cable-Based (ECP) Freight Brake Systems, S-4200 section 3.3.2.1 of the AAR Manual of Standards and Recommended Practices.

3.3.3.3 Broadcast Exception In

A CCD should respond to a broadcast exception message in accordance with the , S-4200 section 3.3.2 of the AAR Manual of Standards and Recommended Practices.

3.3.3.4 Vehicle ID In

Receiving a Vehicle ID In message causes the CCD to overwrite its vehicle identification information with the information contained within the message.

3.3.3.5 Vehicle Fixed Information

Fixed information which affects the braking performance of a CCD can be updated using the vehicle information message. In order to preserve this information in the event of a power loss, this data is stored in the CCD as a configuration class network variable.

3.3.3.5.1 Contents of the Vehicle Fixed Information Message

The Vehicle information message uses the following data structure:

```
typedef struct vehicle_data
{
int             brake_constant;
unsigned long   loaded_weight;
int             empty_weight;
} vehicle_data;
```

field descriptions for **vehicle_data**:

- **brake_constant** in units of inches^2.
- **loaded_weight** is the gross loaded weight in Kips.
- **empty_weight** in Kips.

3.3.3.6 Vehicle Configuration

When a vehicle configuration message is received a CCD must overwrite its existing configuration with the new data.

3.3.3.7 Train Configuration

When a train configuration message is received a CCD must use this configuration instead of its default vehicle configuration.

3.3.3.8 Time Synch

When a Time Synch message is received by a CCD it should set its internal clock to correspond with the time contained within the message.

3.3.3.9 Change CCD Status

When a change CCD status message is received by a CCD, the receiving CCD must comply and perform as required by the new status.

3.3.3.10 Exception Update Request

A CCD should respond to an Exception update request by sending an exception update message to the HEU for the exception code contained within the exception update request.

3.3.4 Network Image Definition for the CCD

Domain Table

index	id[DOMAIN_ID_LEN]	subnet	node	len	key
0	-	set @ install	set @ install	0	0

- All CCDs are members of one domain.
- Only one domain exists in the Train Control Network therefore zero length domain length is used.
- Authenticated services are not used.

CCD Addr Table

Index	type	grp type	size	domain	backlog	node	member	rpt_timer	retry	rcv_timer	tx_timer	group	subnet
0 (b cast)	3	0	0	0	1	n/a	0	1 (24 mS)	0	3 (384 ms)	9 (384 ms)	0	0
1 (s/n to HEU)	1	0	n/a	0	n/a	1	n/a	8 (256 mS)	3	3 (384 ms)	9 (384 ms)	n/a	1

- All *basic* messages from the CCD are domain wide broadcast, or addressed for the lead HEU.

CCD Network Variable Configuration Table

NV Name	SD String	Priority	Direction	Hi Sel	Low Sel	Turn Around	Service	Addr Index
HEU Beacon	"@ccdl01.heu_beacon_in"	yes	in	0x00	0x00	no	-	15
EOT Beacon	"@ccdl02.eot_beacon_in	yes	in	0x00	0x01	no	-	15
Status	"@ccdl03.status_out"	no	out	0x00	0x02	no	2 (UNACKD)	1 (s/n to HEU)
Exception	"@ccdl04.except_out"	no	out	0x00	0x03	no	0 (ACKD)	1 (s/n to HEU)
B.Cast Except In	"@ccdl05.bcast_except_in"	no	in	0x00	0x04	no	-	15
B.Cast Except Out	"@ccdl06.bcast_except_out"	no	out	0x00	0x04	no	2 (UNACKD)	0 (b.cast)
Vehicle ID Out	"@ccdl07.vehicle_info_out"	no	out	0x00	0x05	no	0 (ACKD)	1 (s/n to HEU)
Vehicle ID In	"@ccdl08.vehicle_info_in"	no	in	0x3F	0xF9	no	-	15
Vehicle Config	"@ccdl09.vehicle_config_in"	no	in	0x3F	0xF8	no	-	15
Time Synch	"@ccdl10.time_synch_in"	no	in	0x00	0x0A	no	-	15
Change CCD Status	"@ccdl11.change_ccd_in"	no	in	0x3F	0xF6	no	-	15
Exception Update	"@ccdl12.except_update_out"	no	out	0x00	0x06	no	0 (ACKD)	1 (s/n to HEU)
Vehicle Data	"@ccdl13.vehicle_info_out"	no	out	0x00	0x07	no	0 (ACKD)	1 (s/n to HEU)
Excpt. Update RQ.	"@ccdl14.excpt_updt_rq_in"	no	in	0x3F	0xF2	no	-	15
Train Config In	"@ccdl15.train_config_in"	no	in	0x00	0x09	no	-	15

- Bound ECP brake network variables use selector range 0x0000 to 0x0FFF.
- Unbound network variables use selector range 0x3000 to 0x3FFF

3.4 The End of Train Device (EOT)

3.4.1 Function of the EOT

The purpose of the EOT is to assure continuity of the electric trainline cable and continuity of the air supply pipe. Only one EOT device may be active in train.

3.4.2 EOT Output Messages

3.4.2.1 EOT Beacon

3.4.2.1.1 Contents of the EOT Beacon

The EOT data structure is used for the EOT beacon message.

```
typedef struct eot_data_struct
     {
      unsigned    status;
      unsigned    brake_pipe_pressure;
      unsigned    battery_volts;
      } eot_data_struct;
```

Field Descriptions:

- **status** is the current status of the EOT. Status is a bit field which uses the following definition:

status

bit	Definition
A (LSB)	0 = power off, 1 = power on
B	0 = marker off, 1 = marker on
C	0 = blue flag off, 1 = blue flag on
D	0 = train stopped, 1 = train moving
E	spare
F	spare
G	spare
H	spare

- **brake_pipe_pressure** in PSIG with one (1) PSI resolution.
- **battery_volts** with one tenth (0.1) volt resolution.

3.4.2.1.2 Frequency of the EOT Beacon

The EOT beacon is transmitted once per second.

3.4.2.2 Exception Message

The exception message is used to transmit information to another node(s) within the network. Only conditions which need to be logged or acted upon should generate an exception message. Appendix A contains a list of defined exception codes, priorities for the exception, and what devices should receive the exception message. A unicast exception should be acknowledged, but a broadcast exception should not be acknowledged.

3.4.2.2.1 Contents of Exception Message

The exception code structure is used by the following messages:

- (EOT) Exception
- (EOT) Broadcast Exception

```
typedef struct exception_code_struct
    {
    char            ccd_id[11];
    unsigned  long  code;
    unsigned  long  data;
    int             priority;
    };
```

Field Descriptions:

- **ccd_id** is the ID of the device generating the exception (car reporting mark).
- **code** is the exception code. A list of defined codes is provided in appendix A
- **data** is additional data which may be required by the HEU.

- **priority** Indicates the severity of the exception, and the recommended action which should be taken.

Priority

Code	**Description**
0	exception clear
1	train must be stopped emergency rate
2	train must be stopped immediately at service rate
3	train must be stopped immediately at service rate if three or more like messages of this priority are received within 10 seconds.
4	reduced speed to next convenient point
5	maintenance required at next terminal
6	maintenance required at destination terminal
7	record and notify operator a CCD is cutout
8	record only
9	Event / No need to clear.

3.4.2.2.2 Frequency of Exception Message

Exception messages are transmitted on an as needed basis. Once an exception is transmitted from a node, it is not retransmitted unless the priority of the condition changes.

3.4.2.3 Exception Update

When an unknown exception code is sent to the HEU, the HEU may request an exception code update from the sending node. The response to the exception update request is the exception update message.

3.4.2.3.1 Contents of Exception Update

The data structure for the exception code update is:

```
typedef struct exception_update
     {
      unsigned long code;
      char                description[28];
      } exception update;
```

Field Descriptions:

- **code** is the exception code number.
- **description** is a string up to twenty-eight (28) characters in length. This contains a description of the code.

3.4.2.3.2 Frequency of Exception Update

The Exception update message is transmitted on an as needed basis.

3.4.3 Input Messages for the EOT

3.4.3.1 Time Synchronization

When a Time Synch message is received by the EOT it should set its internal clock to correspond with the time contained within the message.

3.4.3.2 EOT Command

When an EOT command message is received, the EOT must change its operation to comply with the command message.

3.4.3.3 HEU Beacon

The HEU beacon is used by the EOT to check the continuity of the trainline. The EOT should respond to a failure to receive the HEU beacon in accordance with S-4200 of the AAR Manual of Standards and Recommended Practices.

3.4.3.4 Broadcast Exception In

An EOT should respond to a broadcast exception message in accordance with S-4200 of the AAR Manual of Standards and Recommended Practices.

3.4.3.5 Exception Update Request

An EOT should respond to an Exception Update Request by sending an exception update message to the HEU for the exception code contained within the exception update request.

3.4.4 Network Image Definition for the EOT

Domain Table

index	id[DOMAIN_ID_LEN]	subnet	node	len	key
0	-	set @ install	set @ install	0	0

- The EOT is only a member of one domain.
- Only one domain exists in the Train Control Network therefore zero length domain length is used.
- The EOT is always subnet 1 and node 2.
- Authenticated services are not used.

EOT Addr Table

Index	type	grp type	size	domain	backlog	node	member	rpt_timer	retry	rcv_timer	tx_timer	group	subnet
0 (b cast)	3	0	0	0	1	n/a	0	1 (24 mS)	0	3 (384 ms)	9 (384 ms)	0	0
1 (s/n to HEU)	1	0	n/a	0	n/a	1	n/a	8 (256 mS)	3	3 (384 ms)	9 (384 ms)	n/a	1

- All *basic* messages from the EOT are domain wide broadcast.

EOT Network Variable Configuration Table

NV Name	SD String	Priority	Direction	Hi Sel	Low Sel	Turn Around	Service	Addr Index
EOT Beacon	"@eotl01.eot_beacon_out"	yes	out	0x00	0x01	no	2 (UNACKD)	0 (b.cast)
Time Synch	"@eotl02.time_synch_in"	no	in	0x00	0x0A	no	-	15
EOT Command	"@eotl03.eot_command_in"	no	in	0x00	0x08	no	-	15
Exception	"@eotl04.except_out"	no	out	0x00	0x03	no	0 (ACKD)	1 (s/n to HEU)
Exception Update	"@eotl05.except_update_out"	no	out	0x00	0x06	no	0 (ACKD)	1 (s/n to HEU)
Excpt. Update RQ.	"@eotl06.excpt_updt_rq_in"	no	in	0x3F	0xF2	no	-	15
B.Cast Except Out	"@eotl07.bcast_except_out"	no	out	0x00	0x04	no	2 (UNACKD)	0 (b.cast)
B Cast Except In	"@eotl08.bcast_except_in"	no	in	0x00	0x04	no	-	15
HEU Beacon In	"@eotl09 heu_beacon_in"	yes	in	0x00	0x00	no	-	15

- Bound ECP brake network variables use selector range 0x0000 to 0x0FFF.
- Unbound network variables use selector range 0x3000 to 0x3FFF.

3.5 The Power Supply Controller (PSC)

3.5.1 Function of the Power Supply Controller

The purpose of the power supply controller (PSC) is to allow network based control of the trainline power supplies. This device is also used to prevent the power from being applied to the electric trainline while vehicles are being added or removed from the train. No more than one power supply controller is allowed per locomotive.

3.5.2 Power Supply Controller Output Messages

3.5.2.1 Exception Message

The exception message is used to transmit information to another node(s) within the network. Only conditions which need to be logged or acted upon should generate an exception message. Appendix A contains a list of defined exception codes, priorities for the exception, and what devices should receive the exception message. A unicast exception should be acknowledged, but a broadcast exception should not be acknowledged.

3.5.2.1.1 Contents of Exception Message

The exception code structure is used by the PSC exception message:

```
typedef struct exception_code_struct
    {
    char            ccd_id[11];
    unsigned  long  code;
    unsigned  long  data;
    int             priority;
    };
```

Field Descriptions:

- **ccd_id** is the ID of the device generating the exception (car reporting mark).
- **code** is the exception code. A list of defined codes is provided in appendix A
- **data** is additional data which may be required by the HEU.

- **priority** Indicates the severity of the exception, and the recommended action which should be taken.

Priority

Code	**Description**
0	exception clear
1	train must be stopped emergency rate
2	train must be stopped immediately at service rate
3	train must be stopped immediately at service rate if three or more like messages of this priority are received within 10 seconds.
4	reduced speed to next convenient point
5	maintenance required at next terminal
6	maintenance required at destination terminal
7	record and notify operator a CCD is cutout
8	record only
9	Event / No need to clear.

3.5.2.1.2 Frequency of Exception Message

Exception messages are transmitted on an as needed basis. Once an exception is transmitted from a node, it is not retransmitted unless the priority of the condition changes.

3.5.3 Input Messages for the PSC

3.5.3.1 HEU Beacon

The PSC should not allow the power supply to provide an output voltage until the HEU Beacon is received. This function overrides any command from the HEU. Also, if the HEU beacon is missed for three consecutive seconds the PSC should turn the power supply output off.

3.5.3.2 Time Synch

When a Time Synch message is received by the EOT it should set its internal clock to correspond with the time contained within the message.

3.5.3.3 Power Supply Enable

When the power supply enable message is received the PSC should enable or disable the power supply accordingly. If no power supply enable message is received then the PSC assumes a default of "power supply disabled."

3.5.3.4 Power Switch

When the power switch enabled is received the PSC should activate or deactivate the power supply accordingly. Note that the power supply may not be activated until the EOT beacon is received and a power on message from the HEU is received.

3.5.4 Network Image for the Power Supply Controller

Domain Table

index	id[DOMAIN_ID_LEN]	subnet	node	len	key
0	-	set @ install	set @ install	0	0

- All PSCs are members of one domain.
- Only one domain exists in the Train Control Network therefore zero length domain length is used.
- Authenticated services are not used.

PSC Addr Table

Index	type	grp type	size	domain	backlog	node	member	rpt_timer	retry	rcv_timer	tx_timer	group	subnet
0 (s/n to HEU)	1	0	n/a	0	n/a	1	n/a	1 (24 mS)	3	3 (384 ms)	9 (384 ms)	n/a	1

PSC Network Variable Configuration Table

NV Name	SD String	Priority	Direction	Hi Sel	Low Sel	Turn Around	Service	Addr Index
EOT Beacon	"@psci01.eot_beacon_out"	yes	in	0x00	0x01	no	-	15
Time Synch	"@psci02.time_synch_in"	no	in	0x00	0x0A	no	-	15
Power Supply Enable	"@psci03.psc_enable_in"	no	in	0x3F	0xF1	no	-	15
Power Switch	"@psci04.psc_switch_in"	no	in	0x3F	0xF0	no	-	15
Exception	"@psci05.except_out"	no	out	0x00	0x03	no	0 (ACKD)	1 (s/n to HEU)

- Bound ECP brake network variables use selector range 0x0000 to 0x0FFF.
- Unbound network variables use selector range 0x3000 to 0x3FFF.

4.0 STANDARD CAR NETWORK INTERFACE REQUIREMENTS

Provisions for a standard car network interface are contained in S*** section * of the AAR Manual of Standards and Recommended Practices.

5.0 DISTRIBUTED LOCOMOTIVE CONTROL SYSTEM REQUIREMENTS

Provisions for distributed locomotive control are contained in S*** section * of the AAR Manual of Standards and Recommended Practices.

APPENDIX A

EXCEPTION CODES

Exception Number	Exception Description	Priority	Transmission Type
10000	Loss of Communication with HEU	1	Broadcast
10001	Loss of Brake Pipe Pressure	2 or 3	Unicast to HEU
10002	Brake Pipe Not Charging	2 or 3	Unicast to HEU
10010	Loss of Head End Power	2 or 3	Unicast to HEU
10011	Low Head End Power	4	Unicast to HEU
10020	Low Res. Pressure	3	Unicast to HEU
10030	Low Brake Cylinder Pressure	8	Unicast to HEU
10031	High Brake Cylinder Pressure	7	Unicast to HEU
10040	Low Battery Voltage	7	Unicast to HEU
10041	High Battery Voltage	8	Unicast to HEU

APPENDIX B

LONWORKS STANDARD NETWORK VARIABLE LIST

A6 FAA REGULATIONS

FAA regulations are an example of how design neutral performance based regulations can be written and implemented. It should be pointed out, however, that the requirements for aircraft safety are much more stringent than those for ground vehicles. When an aircraft is in flight, all systems must remain operational while a ground vehicle can simply be stopped or put into "limp mode". Nevertheless, reviewing the FAA regulations can provide insight into the nature of fail-safe requirements and procedures for complex systems involving electronics software and communications.

Below are excerpts from the Federal Aviation Administrations Special Federal Aviation Regulation No. 13 : *Airworthiness Standards for Transport Airplanes.*

Sec. 25.1431 Electronic equipment

(a) In showing compliance with Sec. 25.1309 (a) and (b) with respect to radio and electronic equipment and their installations, critical environmental conditions must be considered.

(b) Radio and electronic equipment must be supplied with power under the requirements of Sec. 25.1355(c).

(c) Radio and electronic equipment, controls, and wiring must be installed so that operation of any one unit or system of units will not adversely affect the simultaneous operation of any other radio or electronic unit, or system of units, required by this chapter.

Sec. 25.1309 Equipment, systems, and installations

(a) The equipment, systems, and installations whose functioning is required by this subchapter, must be designed to ensure that they perform their intended functions under any foreseeable operating condition.

(b) The airplane systems and associated components, considered separately and in relation to other systems, must be designed so that--

(1) The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable, and

(2) The occurrence of any other failure conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions is improbable.

(c) Warning information must be provided to alert the crew to unsafe system operating conditions, and to enable them to take appropriate corrective action. Systems, controls, and associated monitoring and warning means must be designed to minimize crew errors which could create additional hazards.

(d) Compliance with the requirements of paragraph (b) of this section must

be shown by analysis, and where necessary, by appropriate ground, flight, or simulator tests. The analysis must consider--

(1) Possible modes of failure, including malfunctions and damage from external sources.

(2) The probability of multiple failures and undetected failures.

(3) The resulting effects on the airplane and occupants, considering the stage of flight and operating conditions, and

(4) The crew warning cues, corrective action required, and the capability, of detecting faults.

(e) Each installation whose functioning is required by this subchapter, and that requires a power supply, is an "essential load" on the power supply. The power sources and the system must be able to supply the following power loads in probable operating combinations and for probable durations:

(1) Loads connected to the system with the system functioning normally.

(2) Essential loads, after failure of any one prime mover, power converter, or energy storage device.

(3) Essential loads after failure of--

(i) Any one engine on two-engine airplanes; and

(ii) Any two engines on three-or-more-engine airplanes.

(4) Essential loads for which an alternate source of power is required by this chapter, after any failure or malfunction in any one power supply system, distribution system, or other utilization system.

(f) In determining compliance with paragraphs (e) (2) and (3) of this section, the power loads may be assumed to be reduced under a monitoring procedure consistent with safety in the kinds of operation authorized. Loads not required in controlled flight need not be considered for the two-engine-inoperative condition on airplanes with three or more engines.

(g) In showing compliance with paragraphs (a) and (b) of this section with regard to the electrical system and equipment design and installation, critical environmental conditions must be considered. For electrical generation, distribution, and utilization equipment required by or used in complying with this chapter, except equipment covered by Technical Standard Orders containing environmental test procedures, the ability to provide continuous, safe service under foreseeable environmental conditions may be shown by environmental tests, design analysis, or reference to previous comparable service experience on other aircraft.

[Amdt. 25-23, 35 FR 5679, Apr. 8, 1970, as amended by Amdt. 25-38, 41 FR 55467, Dec. 20, 1976; Amdt. 25-41, 42 FR 36970, July 18, 1977]

Sec. 25.1355 Distribution system.

(a) The distribution system includes the distribution busses, their associated feeders, and each control and protective device.

(b) [Reserved]

(c) If two independent sources of electrical power for particular equipment or systems are required by this chapter, in the event of the failure of one power source for such equipment or system, another power source (including its separate feeder) must be automatically provided or be manually selectable to maintain equipment or system operation.

[Doc. No. 5066, 29 FR 18291, Dec. 24, 1964, as amended by Amdt. 25-23, 35 FR 5679, Apr. 8, 1970; Amdt. 25-38, 41 FR 55468, Dec. 20, 1976]

Sec. 25.1363 Electrical system tests

(a) When laboratory tests of the electrical system are conducted--

(1) The tests must be performed on a mock-up using the same generating equipment used in the airplane;

(2) The equipment must simulate the electrical characteristics of the distribution wiring and connected loads to the extent necessary for valid test results; and

(3) Laboratory generator drives must simulate the actual prime movers on the airplane with respect to their reaction to generator loading, including loading due to faults.

(b) For each flight condition that cannot be simulated adequately in the laboratory or by ground tests on the airplane, flight tests must be made.

Sec. 25.1357 Circuit protective devices.

(a) Automatic protective devices must be used to minimize distress to the electrical system and hazard to the airplane in the event of wiring faults or serious malfunction of the system or connected equipment.

(b) The protective and control devices in the generating system must be designed to de-energize and disconnect faulty power sources and power transmission equipment from their associated busses with sufficient rapidity to provide protection from hazardous over-voltage and other malfunctioning.

(c) Each resettable circuit protective device must be designed so that, when an overload or circuit fault exists, it will open the circuit irrespective of the position of the operating control.

(d) If the ability to reset a circuit breaker or replace a fuse is

essential to safety in flight, that circuit breaker or fuse must be located and identified so that it can be readily reset or replaced in flight.

(e) Each circuit for essential loads must have individual circuit protection. However, individual protection for each circuit in an essential load system (such as each position light circuit in a system) is not required.

(f) If fuses are used, there must be spare fuses for use in flight equal to at least 50 percent of the number of fuses of each rating required for complete circuit protection.

(g) Automatic reset circuit breakers may be used as integral protectors for electrical equipment (such as thermal cut-outs) if there is circuit protection to protect the cable to the equipment.

A7 EUROPEAN REGULATIONS

A4.1 Overview of ECE Braking Regulations

The regulation for heavy vehicle brakes is ECE 324 R-13. This "type approval" sytle regulation has three main features:

1) an approval process

2) brake system specifications

3) brake performance tests

Each of these regulatory components are discussed below.

Approval process

The approval process for braking systems under rR13 is quite complex. A complete component level design specification must be submitted to the authorizing body for its review. The authority examines the regulation with regard to compliance with the brake system specifications (Brake system specifications are discussed in the following section). The authority is also responsible for carrying out the brake performance tests.

Excerpts from ECE 324 R-13 related to Approval

3.1. The application for approval of a vehicle type with regard to braking shall be submitted by the vehicle manufacturer or by his duly accredited representative.

3.2. It shall be accompanied by the undermentioned documents in triplicate and by the following particulars:

3.2.1. a description of the vehicle type with regard to the items specified in paragraph 2.2. above. The numbers and/or symbols identifying the vehicle type and, in the case of power-driven vehicles, the engine type shall be specified;

3.2.2. a list of the components, duly identified, constituting the braking system;

3.2.3. a diagram of assembled braking system and an indication of the position of its components on the vehicle;

3.2.4. detailed drawings of each component to enable it to be easily located and identified.

3.3. A vehicle, representative of the vehicle type to be approved, shall be submitted to the Technical Service conducting the approval tests.

3.4. The competent authority shall verify the existence of satisfactory arrangements for ensuring effective control of the conformity of production before type approval is granted.

Brake system specifications

ECE motor vehicle regulation are intended to be as design neutral as possible. The regulation specifies requirements for the system and various components but does not, for the most part, specify how these requirements are to be achieved. However, a number of design specific items are included in the regulation for features such as tractor trailer compatibility and indicator lamps for the driver. In addition, specific requirements are in place to related to fault tolerance and failure modes. The many specifications for failure modes often anticipate a particular design feature. A relatively large section of the brake specifications are such conditional items beginning with the word "If".

Examples of system requirements from ECE 324 R-13 are given below.

Example performance specifications

5.1.1.1. The braking system shall be so designed, constructed and fitted as to enable the vehicle in normal use, despite the vibration to which it may be subjected, to comply with the provisions of this Regulation.

5.1.1.2. In particular, the braking system shall be so designed, constructed and fitted as to be able to resist the corroding and ageing phenomena to which it is exposed.

5.1.2.1. Service braking system

The service braking system must make it possible to control the movement of the vehicle and to halt it safely, speedily and effectively, whatever its speed and load, on any up or down gradient. It must be possible to graduate this braking action. The driver must be able to achieve this braking action from his driving seat without removing his hands from the steering control.

5.1.2.2. Secondary braking system

The secondary braking system must make it possible to halt the vehicle within a reasonable distance in the event of failure of the service braking system. It must be possible to graduate this braking action. The driver must be able to obtain this braking action from his driving seat while keeping at least one hand on the steering

control. For the purposes of these provisions it is assumed that not more than one failure of the service braking system can occur at one time.

Example compatibility specifications

5.1.2.4. Pneumatic connections between power-driven vehicles and trailers.

In the case of a braking system operated by compressed-air, the pneumatic link with the trailer must be of the type with two or more lines. However, in all cases, all the requirements of this Regulation must be satisfied by the use of only two lines. Shut-off devices which are not automatically actuated shall not be permitted.

In the case of tractor and semi-trailer combinations, the flexible hoses shall be a part of the tractor vehicle. In all other cases, the flexible hoses shall be a part of the trailer.

Example driver interface specifications

5.2.1.4.2. The failure of a part of a hydraulic transmission system shall be signaled to the driver by a device comprising a red tell-tale lamp lighting up not later than on actuation of the control and remaining lit as long as the failure persists and the ignition (start) switch is in the "on" (run) position. However, a device comprising a red tell-tale lamp lighting up when the fluid in the reservoir is below a certain level specified by the manufacturer is permitted. The tell-tale lamp must be visible even by daylight; the satisfactory condition of the lamp must be easily verifiable by the driver from the

driver's seat. The failure of a component of the device must not entail total loss of the braking system's effectiveness.

Example Failure mode specifications

5.2.1.2.1. There must be at least two controls, independent of each other and readily accessible to the driver from his normal driving position.

For all categories of vehicles, except M_2 and M_3, every brake control (excluding a retarder control) shall be designed such that it returns to the fully off position when released. This requirement shall not apply to a parking brake control (or that part of a combined control) when it is mechanically locked in an applied position;

5.2.1.2.2. the control of the service braking system must be independent of the control of the parking braking system;

5.2.1.2.3. if the service braking system and the secondary braking system have the same control, the effectiveness of the linkage between that control and the different components of the transmission systems must not be liable to diminish after a certain period of use;

5.2.1.2.4. if the service braking system and the secondary braking system have the same control, the parking braking system must be so designed that it can be actuated when the vehicle is in motion. This requirement shall not apply if the vehicle's service braking system can be actuated, even partially, by means of an auxiliary control;

5.2.1.2.5. in the event of breakage of any component other than the brakes (as defined in paragraph 2.6. of this Regulation) or the components referred to in paragraph 5.2.1.2.7. below, or of any other failure of the service braking system (malfunction, partial or total exhaustion of an energy reserve), the secondary braking system or that part of the service braking system which is not affected by the failure, must be able to bring the vehicle to a halt in the conditions prescribed for secondary braking;

5.2.1.2.6. In particular, where the secondary braking system and the service braking system have a common control and a common transmission:

5.2.1.2.6.1. if service braking is ensured by the action of the driver's muscular energy assisted by one or more energy reserves, secondary braking must, in the event of failure of that assistance, be capable of being ensured by the driver's muscular energy assisted by the energy reserves, if any, which are unaffected by the failure, the force applied to the control not exceeding the prescribed maxima;

5.2.1.2.6.2. if the service braking force and transmission depend exclusively on the use, controlled by the driver, of an energy reserve, there must be at least two completely independent energy reserves, each provided with its own transmission likewise independent; each of them may act on the brakes of only two or more wheels so selected as to be capable of ensuring by themselves the prescribed degree of secondary braking without endangering the stability of the vehicle during braking; in addition, each of the aforesaid energy reserves must be equipped with a warning device as defined in paragraph 5.2.1.13. below;

Braking system performance tests

ECE 324 R-13 includes an set performance tests that must be passed before approval is obtained. The tests are quite extensive and cover al aspects of the brake systems performance. These tests consider:

- Stopping performance for:
  - Normal road adhesion
  - Reduced road adhesion
  - Cold brakes
  - Hot brakes
  - Flat surface conditions
  - Down hill conditions
  - Loaded trailers
  - Unloaded trailers
- Braking rate of trailer
- Response time
- Capacity of air reservoirs
- Brake distribution tests
- Antilock brake performance

A4.2 FUTURE DIRECTION FOR ECE REGULATIONS.

Work is underway within the ECE to produce a method for self compliance for Motor vehicle regulations. The current proposal is to develop an ISO 9000 process for self compliance. The ISO 9000 process would specify in great detail the procedure for caring out each compliance test. It would also specify documentation associated with each test. Within this framework each truck manufacturers would be audited by an ECE authority (member country) for ISO 9000 compliance. Once a company is compliant it may then use the prescribed process to self certify its products.

A second initiative within ECE is the concept of functional equivalence. This concept if realized would produce a means for moving to a more design neutral regulation. This initiative has begun very recently and is not well defined. Self compliance is the first priority. The concept of functional equivalence will be pursued only after self compliance is achieved.

Changes to ECE R13 for ECBS

The following is a report produced by the Heavy Duty Brake Manufactures regarding recent changes to ECE-R13 related to **ECBS**.

"ELECTRONICALLY CONTROLLED BRAKING SYSTEMS" - ECBS

United Nations ECE Regulation No. 13 has recently been amended to cater for ECBS on motor vehicles and on trailers; the relevant specifications are in doc. TRANS/WP.29/505 dated 9 July 1996 (Supplement 2 to the 09 Series of Amendments to ECE Regulation No. 13).

Supplement 2 to the 09 Series of Amendments will enter into force on 22 February 1997. This is the date when vehicle manufacturers may apply for type-approval of vehicles with ECBS. From 1 October 1998, any vehicle with ECBS submitted for a new type-approval must meet the 09 "Supplement 2" specifications. There will be a third date (in 2000 or later), when existing type-approvals must be updated to the 09 level.

The above specifications for ECBS were initiated in 1989 by a committee of industry experts and subsequently elaborated within 11 meetings of a joint government/industry Working Group.

The final specifications were approved by the GRRF committee in December 1995 and adopted by the senior WP.29 committee in June 1996 for official inclusion within ECE Regulation No. 13.

PRINCIPLES

The following principles were agreed for the introduction of ECBS into ECE Regulation No. 13 (R.13):

1. Vehicles with ECBS should not be subject to more stringent performance demands than vehicles without ECBS, e.g., the same stopping distances should be applicable.

   NB. This would be a starting point; like with ABS (Antilock Braking Systems), more stringent specifications may be introduced later.

2. The same safety requirements (secondary/residual performance and failure indication) should apply to vehicles with ECBS as to vehicles without ECBS.

   NB. Electronic controls may give rise to new types of faults, errors, and malfunctions which require special consideration, e.g., serial data bus communication faults.

3. Electronic control of the braking system should be considered as an optional alternative to current hydraulic, pneumatic or combined control systems; i.e., ECBS should not be mandatory for any vehicle category.

4. All potential electronic control solutions should be taken into account, from the simplest partial electronic devices to the most sophisticated fully electronic control systems.

5. Further technical developments should not be inhibited.

6. The ECBS specifications should be integrated within the present Regulation. They should not be added within a separate Annex, as for ABS in Annex 13 to R.13.

7. Compatibility between old and new towing vehicles and trailers should be ensured, or adequate warning provided to the driver.

The technical content of doc.TRANS/WP.29/505 may be summarized as follows:

A) SERVICE BRAKING WITH ECBS

It shall be possible to apply the service brakes after the ignition has been switched off.

A failure in the electric wiring (breakage, disconnection) of the control systems shall ensure that the residual and secondary (and trailer) performance can be achieved and be indicated to the driver. The same conditions apply to a deterioration of the battery energy; an alternator failure shall ensure at least 20 full service brake applications.

Auxiliary electrical equipment (lights, wipers) shall not affect the service braking performance.

B) BRAKE FAILURE AND DEFECT WARNING INDICATOR LIGHTS

The numerous features of ECBS and the multitude of electronic failure modes has been recognized by differentiating between minor defects which do not affect the service brake performance (yellow light) and major failures which do (red light). Dynamic faults shall be memorized for static indication. The same philosophy has been extended to trailers with ECBS; minor defects will be indicated by a second yellow light and major failures by the primary red light together with the second yellow light.

C) ELECTRIC PARKING BRAKES

It shall be possible to apply the parking brake after the ignition has been switched off, but release shall be prevented. A failure in the electric wiring shall be indicated to the driver, and subsequently allow the parking brake to be applied and released.

D) TRACTOR/TRAILER COMPATIBILITY

The connections between towing vehicles and trailers shall comprise one pneumatic supply line and one or two control lines, which may be pneumatic and/or electric. Vehicles with only the electric control line will not be type-approved until the reliability of such systems has been confirmed in service. Furthermore, when such vehicles are coupled to vehicles with only the pneumatic control line, then the driver shall be warned and the brakes on one of the vehicles shall be automatically applied.

E) ELECTRONIC AUTOMATIC COMPENSATION

Various forms of compensation, including "coupling force control," are specifically permitted; however, either a failure of such sub-systems or an excessive amount of compensation, shall be indicated to the driver by the yellow light.

F) SERIAL DATA COMMUNICATION

Provision has been made for use of the Bosch CAN system as specified in ISO.11992 for the interface of towing vehicles and trailers to ensure interchangeability.

The data will be transmitted via the 2 free pins on the ISO.7638 ABS electrical connector to provide trailer braking control and additional failure warning to the driver.

G) TRAILERS WITH ECBS

Similar provisions apply to trailers.