FINAL REPORT
Failure Modes, Effects, and Criticality Analysis for AAR S-4200 Cable-Based Electronically Controlled Pneumatic Brake Systems
Revision 0, Dated April 1, 1999

by
The FMECA Team

Composed and Edited by
David E. Limbert and Michael H. deLeon
DEL Engineering
282 Notch Road
Hiram, ME 04041-3431

for
Transportation Technology Center, Inc.
55500 DOT Road
P.O. Box 11130
Pueblo, CO 81001-0130

July 19, 1999
# TABLE OF CONTENTS

## INTRODUCTION
- The FMECA Team 1
- The FMECA Process 1

## RESULTS OF ANALYSIS
- Potential Advantages of ECPB Concept Over Conventional 4
- Potential Disadvantages of ECPB Concept 4

## DISCUSSION OF ANALYSIS
- Severity, Occurrence, and Detection Ratings 5
- Safety, Reliability, and Interoperability Issues 7
  1. SWITCH Mode 7
  2. Train-wide CCD Parameters 8
  3. Battery Failures 10
  4. Brake Cylinder Pressure 12
  5. Adjustment to Car Load 13
  6. Incorrect BCP 13
  7. Reservoir Pressure 13
  8. CCD Cut-out 14
  9. Train-line Shock Hazards 15
  10. Operator Interface, Warnings, and Indications 16
  11. Pneumatic Backup 16
  12. Exceptions, Exception-clears, and HEU Fault Handling Hierarchy 16
  13. Recovery from Fault Responses 17
  14. Multiple Lead HEU Detection 17
  15. Vandalism or Sabotage 17
  16. Initialization and Confirmations 17
  17. Miscellaneous 18
  18. Environmental Requirements 18
  19. Interoperability 18
  20. Action 19

## CONCLUSIONS AND RECOMMENDATIONS 19

## DISCLAIMERS 19

## APPENDIX I  Process for ECP Brake System FMECA 23

## APPENDIX II  FMECA Criteria 25
- Severity Evaluation Criteria - the ‘S’ value 25
- Occurrence Evaluation Criteria – the ‘O’ value 26
- Detection Evaluation Criteria – the ‘D’ value 27
- RPN: Risk Priority Number 27

## APPENDIX III  Definitions of Acronyms and Abbreviations 28

## APPENDIX IV  FMECA for Specification S-4200 (April 1, 1999) 29
INTRODUCTION

DEL Engineering was retained by Transportation Technology Center, Inc. (TTCI) to conduct a Failure Modes, Effects, and Criticality Analysis (or FMECA) for the AAR S-4200 Specification of Cable-Based Electronically Controlled Pneumatic (ECP) Brake Systems. The FMECA worksheet is shown in Appendix IV.

FMECA is a method by which failures of a system, process, or product are identified, classified, evaluated, and prioritized. The criticality of a failure mode represents its risk priority in terms of the probability of the failure, the possible severity of consequences, and the effectiveness of the detection mechanisms. The FMECA drives corrective actions to mitigate critical failure modes, including system specification or design modifications. It also helps to ensure that the specification and its related documents appropriately address safety and reliability issues from a system standpoint.

The FMECA Team

This type of analysis is well-suited for team participation from a number of individuals having substantial involvement in the development and application of ECP Brake Systems. D.H. Stamatis\(^1\) was emphatic in this regard: AUnder no circumstances should any FMEA be done with a single individual...An individual may fill out the FMEA form properly, but there will be built-in biases based on the single perspective of the individual conducting that FMEA. A core team was formed from a group that gathered in November 1998 to discuss the approach to use (see Appendix I), the evaluation criteria (see Appendix II), and involve all present in exercises to help them understand the process and the alternate approaches possible for doing the analysis and filling out the FMECA form (see Appendix IV). The core team, which participated in weekly phone conferences, consisted of Fred Carlson and Tom Nast of TTCI, Jim Truglio of New York Air Brake (NYAB), David Halvorson of Westinghouse Air Brake Company (WABCO), and David Limbert and Michael deLeon of DEL Engineering. On occasion other people present at the November meeting would participate in phone conferences, providing helpful input. Those included: John Punwani, Jim Wilson, and Charles Bielitz of the Federal Railroad Administration (FRA), Greg Gagarin of Amtrak, Rick Stauffer of Burlington Northern-Santa Fe (BNSF), Anthony Manconi of Canadian Pacific Railroad (CPR), Jeremy Waldrop of Zeftron, Dale Stevens of NYAB, and David Peltz of GE-Harris.

The FMECA Process

The process that the FMECA team adopted in performing the FMECA is described in Appendix I. Such an analysis can be performed by listing the component blocks of the system (cable, CCDs,

---

identifying their functions, and then proceeding with the failure modes associated with the functions, the effects of those failures, the causes of the failures, and the detection/mitigation built into the system to prevent the ultimate effect from happening. The team chose to use the viewpoint of the specification itself, as the specification lists the functions that the system and its components are to perform. Using this view, the component or components that are involved in the cause for failure are identified under cause. Manufacturers, for their specific designs, may wish to use a component view, where they select the level of component assembly appropriate for their needs. For example, they may select various sub-assemblies and major components within the EOT (pressure transducer, transceiver, battery, battery charger, etc. or sub-parts of these) for their initial listing in their analysis.

Before performing the analysis, the team agreed to numeric ranking criteria for rating the effects of a failure mode in terms of its Severity (S), the causes of the failure in terms of their frequency of Occurrence (O), and the effectiveness of the Detection (D) methods and countermeasures that may exist that could counter or mitigate the potential effects of the failure mode. These ratings of Severity (S), Occurrence (O), and Detection (D) must be thoroughly understood by the reader before drawing any conclusions from the FMECA. Please see Appendix II for these ratings.

It is essential to understand, in all cases, that the mitigation measures identified in the FMECA are those things which are effective at preventing the \textit{ultimate effect} from occurring. They are not, however, effective at preventing the cause or the failure mode itself from occurring. One may observe in certain situations that a mitigating factor can be very effective at reducing the criticality of a high-severity effect by relegating the failure outcome to a slightly lower severity; however, the resulting lower severity may come at the cost of less further mitigation, and the resulting analysis may actually yield a higher overall Risk Priority Number (RPN) than the original failure mode.

A high RPN does not necessarily mean the failure mode is safety-critical. For example, several high values were obtained for train delays due to possible equipment failures where the train delay could not be avoided. Conversely, a low RPN does not necessarily mean the failure mode is not a safety issue. Low RPN values are desirable for safety issues, since a low RPN value indicates that the team believes that either the occurrence rate of the cause is low or that the detection/mitigation specified for the system will be effective in preventing the most serious ultimate effect.

During the analysis, DEL Engineering encouraged the FMECA team to better understand the FMECA process, to be attentive to possible conflicts of interest, and to be careful not to overestimate the reliability of software, computer hardware, and human designers, users, operators, and equipment testers without hard data and thorough testing of such factors. We further felt it important that the FMECA team be cautious and not assume all manufacturers have the same level of competence and focus on quality and reliability as those presently involved. As a result of the aforesaid approach, the team paid more attention to potentially high risk failure modes and effectively worked to address important matters.
The guiding philosophy we adopted is that if the specification can survive such a conservative analysis, there is an increased likelihood that it will be a better specification and that the ECPB system will be reliable in its intended application.

In this report we discuss the outcomes of the FMECA of **AAR Specification S-4200** (Revision 0, adopted April 1, 1999) with respect to safety, reliability, and interoperability issues, the limitations of the analysis - including pertinent disclaimers, and some conclusions and recommendations.

**RESULTS OF ANALYSIS**

DEL Engineering has found the FMECA process to be invaluable in helping identify potential problems early in the system design/architecture stage. This process has driven many of the changes and revisions made to the S-4200 specification since November 1998, some of which were quite important and safety-related. Other changes resulting from the FMECA process related to clarifying the intent of the specification so that any manufacturer could become an informed and potentially successful supplier of ECP Brake equipment. This latter advantage of the FMECA relates to its utility in strengthening the interoperability of equipment.

Overall, the ECPB concept offers the potential for vastly improved performance and reliability over that of the conventional (pneumatic-only) freight train brake system. The benefits of using electronics to control distributed braking systems are far superior to those of pneumatics. (We were among the earliest proponents of electro-pneumatic technology for freight applications and we served an important role in developing concepts and providing input to the prototype strawman specifications for this system at the first Advanced Braking System town meetings held in 1993 and 1994.) However, as failure analysts, it is incumbent upon us to plainly represent concerns relative to safety and reliability.

This report highlights those failure modes in the FMECA which exhibit higher risk priority numbers or which exhibit severity high enough to warrant continued attention. Most of these relate to: using the ECPB system in SWITCH Mode, human error (which may be reduced by good operator interfaces, training, and operating rules), incorrect train-wide parameters, other common-mode causes (such as those that cause many or all cars to cut out in a short time span), and the interaction between the CCD and the pneumatic backup system.

---

We now summarize what we view as the salient advantages and potential disadvantages of ECP Brake systems:

**Potential Advantages of ECPB Concept Over Conventional:**

- gives much faster signal propagation: brakes apply simultaneously throughout train, which reduces or eliminates run-in and reduces transient in-train forces
- affords precise control of BCP (steady-state and transient)
- allows electronically-based load sensing
- provides for graduated braking applications and releases, which translates to better train control, less need for power braking, and better fuel economy
- results in much more efficient use of compressed air (since air not used as a signaling medium)
- renders problems with brake valves, brake pipe, reservoirs, etc. much more likely to be reported to the engineer and crew in a timely manner and result in effective mitigation of problems (e.g., detection of sticking brakes)
- provides a basis for enhanced troubleshooting and diagnostics
- greatly reduces the probability of undesired brake applications (e.g., UDEs) and sticking brakes
- greatly reduces the probability of wheel damage due to sticking brakes or incorrect BCPs
- makes intelligence-based preventive maintenance programs more readily achievable
- reduces probability of coupler, car frame, and lading damage due to in-train forces and slack action
- provides room for future growth in train control via electronic control of other brake apparatus, such as disk brakes, enhanced monitoring functions, possibly blended braking, graded braking (apply different retardation to different parts of train, depending on grades)
- may provide a platform for more advanced train system health monitoring via ECPB system communications network
- improves equipment utilization and overall train performance
- provides for increased safety in case of brake pipe blockage after the system has been filled with air.

**Potential Disadvantages of ECPB Concept:**

- the technology as applied to freight brakes is new (and therefore not mature): there may be some difficult periods of adjustment on the learning curve, as is the case with any new technology; however, the conditional approval process provides a time period to assure safety and reliability are acceptable while minimizing risk
- train-wide parameter errors could become possible causes of train-wide over- or under-braking
- many batteries must be maintained
- depending on the design of the operator interfaces, the sheer number of new warnings, indicators, and brake-related functions could overwhelm engineers and cause confusion and errors (the specification addresses this issue by using exception-based warning, warning at particular percent
operative brake levels rather than warning on individual CCD cut-out, and providing for full service or greater braking for significant faults; it can be further mitigated by good design of such interfaces and appropriate crew training programs)

while ECPB equipment is likely to be simpler pneumatically than conventional brakes, this new equipment adds significant electrical complexity and - along with it - different failure modes

It is our intention in this report to use the FMECA as a basis for highlighting areas requiring caution or careful development. We therefore recommend that the ECPB system manufacturers, equipment qualifying entities, railroads, and operating personnel to pay particular attention to the following issues in DISCUSSION OF ANALYSIS, below.

DISCUSSION OF ANALYSIS

This system or specification level FMECA should be viewed as a first step in an overall safety and reliability assurance process for ECPB systems. We recommend that railroads and manufacturers use FMECA and/or other appropriate safety analysis techniques (including fault tree analysis) in the development of specifications and design and manufacture of ECPB components and systems to assure their safe and reliable operation. While we believe that the major categories of faults that can occur because of failures of modules, assemblies, components, and processes are handled within this FMECA of S-4200, a team consideration of the detail faults of other aspects of the system may bring to light some important items.

Severity, Occurrence, and Detection Ratings:

The ratings of Severity (S), Occurrence (O), and Detection (D) used in the FMECA are based on qualitative and (usually) semi-quantitative estimates from members of the FMECA team. There are some important considerations to note relative to how these ratings were developed:

Severity (S)

(a) We encourage particular attention to failure modes whose severity is 9 or 10 (indicating possible safety hazard) and believe some may be candidates for further, supporting analyses, such as Fault Tree Analysis (FTA). A severity (S) value of 9 was used in a lot of places where, if the failure mode occurs and nothing else responds, a serious accident can happen. (See rankings in Appendix II). The Detect/Mitigate column describes what other responses are built into the system or what actions personnel can take to prevent the failure from reaching its most severe effect.
(b) A severity (S) value of 6 also appears frequently. This appears in those cases where the train is stopped or brought to a stop and it may take some time (e.g. an hour or more) while the cause of the fault is found and the problem is resolved before the train can be moved. These do not indicate safety problems, but represent problems that result in additional cost to the railroads.

Occurrence (O)

(a) The O values reflect the team=s estimates of reliability based on their aggregate experience. In many cases, ratings were estimates made without supporting data. Recommendation: as more experience is gained, update O values in the FMECA to reflect new or more reliable data. For example, the team used an O rating of 3 for most types of CCD failures (except for batteries); the corresponding single CCD failure rate is one every 750,000 train miles. Experiential data may show the particular cause as less frequent or more frequent. As continuing analysis is performed during the development, manufacture, and use of the system, those doing the analysis should continue to be aware of the following items:

(i) reliability of prototype systems, or systems early in development (not yet mature), may not accurately reflect reliability of all such systems at all times; use care in relying on estimates developed from limited experiences.

(ii) reliability of designs and products from particular manufacturers should continue to be used as general estimates, but the team should take into consideration that not all manufacturers= capabilities or quality standards are the same, so that care should be used in applying estimates globally.

(iii) conflicts of interest may exist that could influence the estimates of O values.

(b) As suggested previously, there may be certain cases where particularly critical failure modes may warrant a fault tree analysis. In cases where reliability or safety is a major concern, it may be worthwhile to specify limits on failure rates of certain components in order to maintain the overall occurrence rate of a particular failure mode at an acceptable value.

Detection (D)

Certain mitigators used in the FMECA are beyond the scope of S-4200. These include certification, commissioning, and qualification testing, training of personnel, etc. Without such mitigators, criticality of some failure modes could be significantly affected. Recommendation: we encourage all involved with ECPB to continue to use and further develop these mitigators.
Safety, Reliability, and Interoperability Issues

Through many months of revision of the S-4200 specification, we believe that most critical failure modes have been addressed and mitigated. At this time, we consider that most of the remaining work that could be undertaken to improve safety of ECPB systems to be in a gray area with respect to reducing criticality of their associated failure modes. Without sufficient test data or analysis, it becomes increasingly difficult to assess whether the current specification or proposed alternatives provide less risk. The primary tools to resolve some of this uncertainty are further experience, data, and analysis. When the risk is uncertain, it is usually better to err on the side of caution, and for this reason we discuss some particular failure modes of interest in this report.

There are many other failure modes we believe to be of lesser criticality, and are therefore not discussed herein. Nonetheless, we urge manufacturers and operating personnel to read the FMECA for S-4200, since there may be other failure modes that could be considered in equipment designs and operating procedures.

Most of the items discussed below deal with operational procedures, maintenance or detection of problems, operating rules, etc., because much has been done to assure that the ECPB system hardware and software specification provides for safety and appropriate control by operational personnel. The recommendations should be taken as an appreciation for the value of the approval process, operational rules, and periodic testing that are already in place and which will be expanded upon to encompass this new technology. The issues concerning hardware or software failures are generally considered to result from causes having low probability. There are a few comments related to the writing of the specification itself, which offer suggestions assuring operational compatibility between car and locomotive systems provided by different manufacturers.

1. SWITCH Mode:

Although switching operations using ECPB equipment may be no more hazardous than those using conventional brake equipment, we make the following observations:

(a) Since many of the ECPB automatic fault detection functions are suspended while in SWITCH Mode, failure modes tend to have higher criticality than in RUN Mode. We recommend railroads and operating personnel develop training programs to address the associated issues relative to SWITCH Mode.

(b) We believe there are 3 situations where SWITCH Mode is likely to be used:

(1) at sidings during set-outs and pickups;

(2) on the road when RUN Mode cannot be used at all or cannot be used without a fault-induced stop (in order to move a crippled train to a siding, as operating rules may allow);
(3) in yard switching operations (the team indicated that the ECPB system is not expected to be used much in yard operations; locomotive braking is typically used).

The first two situations could pose additional risk, and we encourage railroads to continue to use appropriate guidelines and operating rules to address these. Depending on the particular situation, it may be appropriate to do one or more of the following: wake up CCDs on cars picked up, do a brake set and release, and power up the train line while underway.

(c) If ECPB systems are used for extended periods of time in SWITCH Mode, there is increased probability that CCDs will use the available battery charge and each will cut-out and relinquish control to pneumatic backup at various times. Since the associated fault detection at the HEU is not available in SWITCH Mode, we encourage personnel to understand this risk and to avoid relying on ECPB without TL power for extended periods.

(d) To provide additional mitigation, manufacturers may consider providing optional warning of CCDs that cut-out or enabling device polling and percent operative brake fault operation in SWITCH mode for railroads that may desire these features.

2. Train-wide CCD Parameters:

   The ECPB system relies on several parameters (brake pipe pressure setpoint, loaded car full service NBR, empty/load) that are downloaded from the HEU to all the CCDs and, if such a parameter is grossly incorrect for the particular train or loading condition, there could be a hazard. While we recognize that the engineer must both enter the incorrect parameter and confirm its value, the possibility of a problem exists. Additionally, even if parameters are both entered and confirmed correctly by the engineer, incorrect parameters could still be sent to CCDs if the HEU fails in a particular (unusual) way. The likelihood of these failure modes having a severe effect depends on many factors. These factors can include: the distance needed to stop the train, the grade, the likelihood that railroads will use default values, and the specification requirement for at least 20 psi full service brake cylinder pressure. As currently specified, the PB does not provide effective mitigation to failure modes associated with train-wide parameter errors. Therefore, we call attention to these failure modes.

   (a) Two scenarios where parameter errors could be hazardous:

   (1) If train integrity and HEU communications to CCDs is maintained:

      * Except for the new function allowing the engineer to increase the empty train load setting to loaded while moving (new S-4200 section 4.2.2.2.4.1), once the train is moving, a full service application must be made for 120 seconds in order for the engineer to enter the
Set-up utility to correct the parameter settings. Even during a fault-induced emergency (resulting from, for example, a vented brake pipe) the CCDs will continue to use the incorrect parameters until they can be changed.

(2) If the train is separated after the erroneous parameter has been sent:

* We expect the CCDs behind the communications break to use the last received (erroneous, in this case) parameter value. In this case, the new function allowing the engineer to change from empty to loaded train will not be effective on the isolated set of cars. Again, they could be underbraked as a result, because they will self-initiate an emergency (i.e., they don’t cut out and don’t relinquish control of BCP to PB) based on the erroneous parameter, so the train may not stop if moving on a hill, even when brake pipe pressure is vented.

Some recommendations:

* The specification currently bounds BPP setpoint at the HEU and minimum full service brake cylinder pressure at the CCD. It may also be desirable to provide additional bounds at the HEU (for NBR) and/or internally at CCDs (BPP setpoint, NBR, etc.) so that a downloaded parameter that is far from normal will not be used or to prompt the engineer if the values fall outside of normal ranges.

* Relative to the train-wide empty/load command, several factors must be considered: (1) the possibility that the command could be selected or transmitted erroneously, (2) the reliability of the train-wide parameter vs. designing ECPB systems to rely on on-board load sensing, which could also fail in certain cases. Related factors should include the intended freight application and the environment in and grades of over which the train will operate. The particular design used for the train-wide empty / load function can influence the reliability of the function (e.g., prevent bit errors or address errors from sending the wrong command). One might argue that having the train default to loaded (and requiring the engineer to deliberately select empty) is a less risky than a train full of on-board load-sensing equipment that may fail because of calibration problems, lack of maintenance, or environmental factors. Opposing arguments may also have validity.

(b) The 120-second configuration command could introduce a hazard if the HEU fails after the train is moving and sends the wrong parameters. The probability of this is likely to be low, however. The causes, effects, and mitigators are similar to those for failure modes described above.
(c) Interchanging locomotives between railroads has been identified as a cause for certain failure modes related to train-wide parameters. We believe railroads should pay special attention to developing operating rules for interchanging locomotives with ECPB equipment if they believe parameter differences may be an important issue. The FMECA team believes that the differences in BPP setpoint and NBR are not as significant as differences due to loading.

3. Battery Failures:

(a) At this juncture, we have identified two critical failure modes related to battery failure:

1. A given train (most likely a unit train) contains many batteries of the same advanced age; these batteries therefore have greatly reduced amp-hour capacity. A loss of TL power could create a hazard if these batteries were incapable of powering devices for long enough to maintain adequate braking capability.

2. A given train has mostly new batteries; if the crew were to rely on the battery backup system for extended periods when TL power is off, there is a possibility of losing a significant number of brakes in a short time span once the first of the set fails.

In both of these scenarios, it is of very high probability that the system will stop the train due to the reduction of operative brakes (in RUN mode only). However the length of time it can hold the train in position is not known and depends on the capacity and state of charge of all remaining batteries. Devices could continue to shut down as more batteries fail. Because this may not be known to the crew, we recommend that appropriate training and operating rules be implemented, and particularly that extended operation on battery backup be avoided.

(b) To ensure backup power is available when needed for sufficient periods of time when TL power is off, we believe battery maintenance and operating procedures to be an important consideration. We therefore recommend the following:

* Preventive maintenance programs should be carried out to replace aging batteries. The replacement period should depend on the conditions under which the battery is used, including the temperature, loading and cycling expected, etc., and the railroads should consult with manufacturers in developing effective guidelines for battery replacement.

* In addition to the battery tests outlined in S-4200, manufacturers could explore technologies that would provide effective battery health monitoring and give ample warning of loss of fully-charged battery capacity (e.g., if battery capacity deteriorates to less than 4 hours, the
system could prompt personnel to replace the battery at the next terminal). Such automated health monitoring might be cost-effective if it serves as a safe substitute for preventive maintenance.

* Railroads may also wish to consult manufacturers about developing guidelines for determining when batteries are fully charged after TL power is applied. Here it may be prudent to require crews to be especially wary of battery backup effectiveness if TL power has been applied for only a short time (especially with equipment that has not been powered up in a long time or which has been operated on battery power for a substantial period without recharging), since the specification requires only 5 minutes= worth of advanced warning of shut down due to battery failure.

* Personnel should limit their use of the ECPB system when TL power is off, or (conversely) make sure the train line is properly energized whenever using the ECPB system.

* Since it is possible for train line voltage to be close to the changeover from train line power to battery power, the switching, changing of loads, and resultant changes in power line voltage may create cycling or other problems for CCD power systems, depending on the design used. It may be possible for the communications network test to detect TL problems that could result in reduced TL voltage.

* The specification, as worded, allows the 5-watt reduced power mode to be used repeatedly. This could result in premature depletion of the batteries (assuming the CCDs need up to 10 watts to operate during this time). Therefore, we make the following recommendations:
  (1) The specification could be reworded to limit 5-watt reduced power mode to 15 minutes in any given hour (or other appropriate interval); and/or
  (2) Training and/or operating rules could be developed to discourage the overuse of the 5-watt mode.

* Cold-weather operation could pose additional challenges to the ECPB system, for the following reasons:
  (1) Older locomotives may have trouble delivering enough electrical power for heaters, ancillary equipment, and heavily-loaded TL power supplies. The provision for use of multiple power supplies on leading and trailing locomotives will usually mitigate the problem for older locomotive systems. (Brake manufacturers are working with locomotive manufacturers to assure new locomotives have sufficient power for ECPB systems.)
  (2) Capacity of CCD batteries typically falls with temperature.
(3) CCDs might require more electrical power to operate normally as temperatures drop (this effect and its severity is design dependent).

Railroads should consider these additional factors in their procedures for operating ECPB systems in very cold weather.

(c) Since the crew may not know the age of batteries, nor their current state of charge (there may not much more than 5-minutes= worth of ECPB brakes available), railroads might consider using the following safe operating guideline (RUN Mode operations): once the train stops due to less than 90% operative brake level while TL power is off, the crew should immediately apply other braking mechanisms (independent, PB, hand brakes), as necessary to secure the train, until the TL power and full ECPB functionality can be restored.

(d) While battery failure poses some risk in RUN Mode, it poses a significantly higher risk in SWITCH Mode since many fault detection functions related to batteries and CCD shutdown are suspended. We recommend that crews be trained and required to energize the TL whenever safe to do so in SWITCH Mode.

4. Brake Cylinder Pressure:
Since a goal of this specification (Section 1.0) is to assure uniform and consistent performance of equipment from different manufacturers, and since such specifications usually provide appropriate bounds on system parameters to assure such compatibility and interoperability, we recommend clarifying requirements related to: (1) the determination or setting of NBR for the train and individual cars, (2) the calculation of full service BCP, (3) the calculation of BCP vs. TBC (or NBR vs. TBC), and (4) the required performance (BCP vs. time) and control of final, steady-state BCP. Specification S-4200, as currently presented, permits substantial leeway in equipment design that could, in rare instances, lead to large in-train forces. We would not expect, however, that equipment would be designed in such a way that widely disparate braking could occur, because some degree of linearity between two or more specified operating points or performance requirements is usually expected. Furthermore, existing rules may provide additional constraints over Sn4200 in setting NBRs. It is the team=s view that the frequency and severity of in-train forces will be less than that for conventional trains and that the approval process will assure appropriate interoperability. Nevertheless, DEL Engineering believes that including some additional bounds in the specification would be desirable.
5. Adjustment to Car Load:

As is the case with conventional braking equipment, failures of on-board load devices or sensors on cars could produce sticking brakes, sliding wheels, slid flats, and (in certain cases) thermal damage to wheels. We encourage railroads to continue appropriate preventive maintenance and/or periodic testing of such devices to provide effective mitigation of these types of failures.

6. Incorrect BCP:

(a) We note that there is a possibility that the HEU will not be apprised of an incorrect BCP deteriorating from marginally incorrect to grossly incorrect. The system concept does not presently call for a CCD to transmit a second, more serious exception if the CCD’s control of BCP gets worse after having sent an initial exception message indicating incorrect. We therefore recommend that the HEU use the CCD status message (in RUN Mode) to determine if the CCD’s operating condition has deteriorated further, until the exception is cleared by the CCD. Manufacturers may wish to use other specific diagnostics to provide further mitigation.

(b) We observe that there may be several causes for an erroneous BCP reading which might result in the HEU’s automatically cutting out a CCD. We also observe that the thresholds specified in S-4200 for the HEU to cut out CCDs could be problematic in the context of allowable pressure transducer tolerances. For example, if the target pressure for a particular brake cylinder were 10 psi, an actual BCP of 12 psi could result in the HEU cutting out the CCD based on BCP 20% too high, since 12 psi is within allowable transducer tolerances (+/- 3 psi). We would expect, however, that reasonable equipment designs would report incorrect BCP only when measured BCP is outside of transducer tolerances. Nonetheless, it may be more appropriate to specify a combination of a +/-3 psi tolerance and a percentage tolerance, where the larger tolerance is to be used as the threshold for cutting out a CCD for incorrect BCP. Furthermore, one might specify a reasonable settling period for pressure before the determination of incorrect is made.

(c) If the CCD’s BCP transducer is used both to control BCP and to detect incorrect BCP, the actual BCP could be incorrect but the CCD might not detect it. Because of this possibility, manufacturers should consider designs that are tolerant of this type of failure.

7. Reservoir Pressure:

(a) Although the low reservoir pressure fault threshold (in RUN Mode) is unlikely to result in excessive in-train forces, it could result in increased stopping distances in cases where a heavy train needs full service or emergency braking. However, we note that this situation is no worse than with conventional brake equipment.
(b) Despite the relatively quick reservoir recharging performance of ECPB systems over conventional braking systems, some failure modes continue to be present for low brake pipe pressure. The engineer should continue to observe the EOT BPP display to be aware of the train=s condition.

8. CCD Cut-out:

(a) We believe that the specification does not explicitly prohibit the HEU from automatically cutting out CCDs for reasons other than incorrect BCP. For this reason, prohibiting the HEU from automatically cutting out CCDs in the following situations should be considered:

1) If CCD is self-initiating an emergency;
2) If HEU is commanding a fault-initiated emergency or full service application;
3) If HEU is commanding an emergency TBC based on the engineer=s brake command input.

Note that this suggestion does not preclude the engineer from commanding individual CCDs to cut out at any time.

(b) Although of very low probability during a safety-critical moment, if an HEU failure causes it to erroneously change the operating mode to CUT-OUT while the train is moving or on a hill, there could be a significant hazard, since the specification requires CCDs to cut out immediately and shut down. The primary mitigator in this situation is that the PB will be available if the engineer chooses to activate it. Manufacturers should continue to recognize the possible risks associated with the train-wide CUT-OUT mode message and use appropriate robust software/hardware designs.

(c) If the branch pipe to a CCD is obstructed (i.e., the cut-out cock is closed or if the pipe is otherwise blocked) after the reservoirs on that car are charged, brake applications or leakage will eventually cause the CCD to be cut-out due to an isolated critical loss of brake pipe pressure as sensed by the CCD. If the pressure in the branch pipe continues to drop, which it could do due to leakage, then the pneumatic backup system will apply the brakes on that car, resulting in a stuck brake. No warning is given to the engineer for such a situation. The possible stuck brake could be detected by having the HEU compare the branch pipe and/or reservoir pressures of this car to those of adjacent cars to determine if the CCD really has an abnormal pressure problem and warn the engineer appropriately: a) if the CCD has low branch pipe pressure and other cars do not, then a potential stuck brake situation exists and the car should have its reservoirs drained until the blockage is removed; or b) if the CCD has low branch pipe and others are close to low, then the train could be brought to a stop by the engineer if he or she suspects the pipe is not recharging adequately. The team believes the occurrence of this failure mode might not be
worth significant design effort to mitigate. An alternative mitigator might be for railroads to train personnel to understand that brakes may be stuck on wherever cut-out CCDs occur. An electronically cut-out CCD should be pneumatically cut out and have its reservoirs drained as soon as it is practicable.

9. Train-line Shock Hazards:

(a) Section 4.4.11 appropriately calls for a warning if hazardous voltage is detected on the train line when it should NOT normally exist (i.e., while the HEU is commanding TL power off). However, we note that there are other ways that hazardous voltage could be present on the train line without personnel expecting it, and for this voltage to be exposed to personnel - connector design notwithstanding. We therefore recommend considering additional mitigation, to the effect that any device (EOT or PSC) detecting significant TL voltage at any time (i.e., not only when the Power Flag is OFF) apprise the HEU (via status messages and/or exceptions, depending on the situation) of a hot train line condition. A TL power indicator light should stay lit the entire time any device detects such voltage. If the normal display of train line power ON/OFF is based on detecting mechanisms (i.e., feedback) rather than on operator selection, this would provide the desired mitigation. There may be some difficult implementation issues, but further consideration of such a hot TL indication may be worthwhile.

(b) Members of the FMECA team have expressed confidence in the safe design of TL connectors and believe this design to be an effective mitigator to shock hazards for many failure modes in the FMECA. We recommend continued collection of data related to connector safety and to consider further mitigation measures should connectors exhibit unanticipated shortcomings. Floating power supplies has also been cited as a mitigation to the shock hazard problem. Should one side or the other of the train line be shorted to a car body, increased risk to those handling the cables and connectors may result. Detection of such shorts may be possible.

(c) In addition to handling connectors, there are other ways for the crew or service personnel to be exposed to hazardous TL voltage, such as when servicing equipment, or if parts of the TL are abraded or damaged. Continued adherence to operating rules in regard to lockout of power sources and training for TL-equipped trains will promote effective safety.

(d) In addition to shock hazards, TL power supplies and the TL itself introduce new potential fire hazards. Power supply designs should (and probably do) include the customary mitigating apparatus - such as fuses, overcurrent protection, thermal protection, etc.
10. Operator Interface, Warnings, and Indications:

(1) To assure consistency of implementation, we recommend creating a matrix of warnings - both audible and visual - and details relative to their initiating faults and what is required to discontinue such warnings.

(2) Reliability, readability, and accuracy of displays are important. Periodic testing and requiring the crew to stop the train if they suspect errant displays or warnings would mitigate related failure modes.

(c) Design of operator interfaces (including controls, displays, audible warnings, indicators, and the related factors of lighting and ergonomics, etc.) plays an important role in safety and reliability of complex systems requiring human interaction. Specification S-4200 does not detail requirements for such interfaces; however, we are aware that there is a group working to develop appropriate standards or auxiliary specifications for these human interfaces. These standards should be adopted and referenced by S-4200.

11. Pneumatic Backup:

There are many places in the FMECA where PB is cited as an effective mitigation to failures of the ECP brake system.

(a) The FMECA of Section 4.3.13, function f7 shows a failure mode of CCDs not being able to relinquish control of BCP to PB because of aging components, etc. The PB apparatus could also fail due to stuck valving - especially if it is not used for prolonged periods. However, this apparatus is likely to be exercised regularly by the normal operating practices for trains parked or cuts set out. We recommend continuation of periodic single car testing to assure PB functionality.

(b) PB functionality should be verified on last car of train wherever possible.

12. Exceptions, Exception-clears, and HEU Fault Handling Hierarchy:

The fault hierarchy tables in the specification should be revised to reflect all of the fault handling processed by the HEU, according to notes we have included in the FMECA form for Section 4.4.
13. Recovery from Fault Responses:

Specification logic could be improved for fault recovery, particularly for multiple critical loss faults. There are cases where recovery from certain unusual faults is not clearly defined. The FMECA form in the Appendix includes a table of faults and recovery therefrom at the top of Sec. 4.4.4 and there are other comments in blocks in related subsections of 4.4.4.

14. Multiple Lead HEU Detection:

The team has verbally proposed to change the detection mechanism from the HEUs to the PSCs. This will add to the chain of detection and responses at each locomotive and increase the possible number of failure modes. The reliability of the response will become the product of a) the reliability of the PSC to detect and respond and b) the reliability of the HEU to receive and respond to the PSC warning. An analysis of this proposal has not been included in the FMECA.

15. Vandalism or Sabotage:

As in most every new computing and electronics application, designers should consider the possibility of electronic sabotage, via introduction of viruses or black boxes into the system, and provide appropriate measures for minimizing this possibility. However, it is to be noted that the probability of such sabotage is low because of the high level of understanding of the design of the system necessary to create such a device or virus. Furthermore, ECPB systems exhibit much less vulnerability to the traditional (and more likely) types of vandalism (such as closed angle cocks) than conventional systems because of the automatic fault detection built into ECPB.

16. Initialization and Confirmations:

(a) During Initialization, the ECPB system may be going from no functionality to full functionality, so full functionality is assured only at the completion of Initialization. This is similar to current practice with conventional equipment except that as CCDs wake up and their reservoirs fill, the CCDs are to come up to full service brake cylinder pressure. Still, crew training and operating rules should, as with conventional systems, ensure that releasing of manual or other braking occur only after appropriate braking functionality has been obtained and RUN or SWITCH mode have been entered.

(b) During Initialization, or shortly thereafter, complete and accurate confirmation that the ECPB system has been set up properly (including number of operative brakes and train-wide braking parameters) is crucial to safety. There are many possible causes for CCDs not to restart, for example, so proper confirmation of operative brakes, as is currently required during initial
terminal tests, continues to be very important. Equipment design, operator interface designs, and training should pay particular attention to this issue.

(c) Since there can be hazards associated with the use of improper car and/or locomotive parameters, in the FMECA we recommend appropriate warnings to the engineer, operating rules, and training for cases where devices cannot obtain proper values for the parameters from their respective ID modules. While this is addressed in the Communications Specification, S-4230, we recommend including the requirement in S-4200.

17. Miscellaneous:

(a) Some inputs to the system are critical; their reliability has a major influence on system reliability, criticality, and safety. These include: speed sensor, brake control input, suppression, acknowledgment button, EOT BPP transducer, etc. The railroads should continue to use appropriate inspection, testing, reporting, and repair of such devices.

(b) Independent (visual or wayside equipment) detection of sticking brakes, will continue to be an important activity, even though such failures are expected to be much less frequent in ECPB systems.

18. Environmental Requirements:

Because environmental conditions could be a common-mode cause of mass failures of ECPB system components, we recommend considering the following additional environmental influences and how they might be mitigated in hardware designs or via qualification tests:

* condensing moisture or icing
* dust, particles, smoke, sand
* water infiltration
* chemical exposure (oils, greases, salt, ozone, etc.)
* electromagnetic compatibility and vulnerability (including electrostatic discharge)

19. Interoperability:

One of the stated goals of S-4200 is to ensure interoperability between manufacturers of different equipment. It is therefore necessary that the specification be very clear, thorough, and consistent inasmuch the specification is a mechanism for communicating requirements, and a lack of such qualities could compromise the stated goal. There are a number of places within S-4200 that could be
further clarified, and we have noted our suggestions and recommendations in bright yellow or gold cells.

20. Action: Items described in the Action column of the FMECA - if undertaken - will tend to reduce risk associated with their corresponding failure modes. Additionally, railroads and manufacturers may find this FMECA (or a similar system-level FMECA) to be valuable as a planning tool or in providing input for training, operating procedures, maintenance programs, etc.

CONCLUSIONS AND RECOMMENDATIONS

We will believe that ECPB technology will yield greatly improved braking performance because of its almost instantaneous signal propagation and better control of brake cylinder pressures, as well as its ability to allow graduated releases. Reliability and safety of ECP brakes are also likely to be better than conventional brakes as a result of automated and instantaneous fault detection and warning functionality. Faster reservoir recharging will also increase efficiency of train operations. To further assure that these qualities are achieved, we make the following recommendations:

1. The Safety, Reliability, and Interoperability Issues presented in this report should be addressed.

2. The specification could be clarified further in a number of sections, and we have included appropriate comments in the FMECA form (yellow or gold colored cells). These comments may be considered to be editorial recommendations for future clarifications or revisions to S-4200.

3. According to Stamatis\(^3\), the system FMEA may be considered finished when all the hardware has been defined and the [system] design is declared frozen. At that point, manufacturers should continue applying a design FMECA or a similar quality and safety assurance process to their detail designs. Therefore, we recommend the continued use of the FMECA process (or some other continuous quality improvement process) by the AAR, manufacturers, and railroads for the life cycle of this braking technology. Evaluation of statistical data, such as that collected on other projects, can be used to update occurrence values for further refinement of this and subsequent failure analyses. This is especially important in cases where RPNs are highly sensitive to changes in O values. For example:

Suppose for a particular HEU failure, an occurrence rating of O=2 is expected. However, experience may show a corresponding failure occurrence rating of 4. This would double the resulting RPN values. This will either drive changes in the specification to improve the detection / mitigation methods, drive changes in design or component selection to reduce the occurrence, and/or, in some cases, provide for cycle testing to assure improved durability.

4. We recommend paying particular attention to failure modes whose RPN values exceed 120 or whose severity ranks 9 or 10. It may be prudent to perform a more detailed fault-tree analysis on certain failure modes which could lead to catastrophic failures of the system, such as collisions or derailments.

5. The FMECA process usually involves examining single-point failures within the system, rather than compound failures, however, the team did evaluate some cases of compound failures. A fault-tree analysis would be useful in identifying probabilities of failures due to compound causes that have severe consequences. Manufacturers may also find fault tree analysis (FTA) useful in identifying probabilities of failures due to compound causes in their designs and helpful in selecting from various design alternatives.

6. Mitigation measures which cite testing such as certification, qualification, commissioning, or single-car tests, and those which cite operating rules, should alert the railroads and the Association of American Railroads that continued diligence is important. If this FMECA is to be deemed valid or authoritative in such cases, each cited mitigation measure must trigger the appropriate actions or programs to assure the mitigation is actually present and at the effectiveness estimated by the D rating for the corresponding failure mode. The team believes that the conditional approval process will be effective in assuring that the mitigation is effective.

We encourage railroads and brake equipment manufacturers to continue to pursue this technology, because the potential benefits of a good implementation of ECPB systems will far outweigh any possible disadvantages they may bring. It is our hope that the issues that the FMECA has brought to light are duly considered and that all involved continue to exercise diligence and sound engineering and operational practice to ensure that this new technology for freight applications achieves its considerable potential. We expect that ECPB systems, if designed, implemented, and maintained properly, will be substantially safer and more reliable than the conventional air brake systems they are intended to replace.
DISCLAIMERS

The FMECA should not be relied upon for a definitive evaluation of risk, hazards, and reliability; indeed, this FMECA should be viewed only as a catalyst for further improvement of the specification and resulting braking systems. Accordingly, DEL Engineering makes no representations or claims whatever relative to the suitability of the current FMECA to definitively predict ECP Brake System reliability, safety, or interoperability between equipment of different manufacturers. While DEL Engineering has found the present FMECA to have been extremely valuable in identifying potential pitfalls, we can by no means claim it to be an exhaustive safety and reliability analysis of the system at this time.
APPENDIX I
Process for ECP Brake System FMECA

1. Accurately and completely describe system and its interactions with other systems and users (specifications, flowcharts, drawings, block or schematic diagrams, etc.).

2. Identify members of FMECA team and bring them together. Record date, time, and attendance, and adopted inputs or changes to FMECA form.

3. Identify major subsystems and components and their interactions.

4. Identify all functions of system and its components.

5. Identify environmental, aging, operational, maintenance, and compatibility influences on reliability.

6. Identify classes of failure of component types (e.g., ways a pressure sensor can fail).

3. Brainstorm failure modes: without regard to failure likelihoods or detection and considering all the foregoing information and asking: "What Can Go Wrong?" (This step must be extremely creative and open-minded. Only later will the potential failure modes be rated in terms of severity, likelihood of occurrence, and probability of detection.) This activity precludes reactive judgment, commentary, or discussion, since any answer could become an important failure mode.

4. Refine failure modes from the brainstorming step. Seek clarification on each idea, then consolidate and organize them for entry into FMECA form.

5. Identify how components or subsystems can fail to interact properly.

6. Identify the potential local effects and ultimate (overall) effects of each failure mode. Possible classification of effects:
   LOCAL:
   - effect on component
   - effect on assembly or subsystem

   ULTIMATE:
   - effect on system
   - deterioration or damage to equipment, increase in unscheduled maintenance or repairs
   - effect on mission reliability (e.g., delivering freight from source to destination on time and with no damage; not interfering with other traffic or train scheduling, etc.)
   - effect on train handling or safety (hazards)

7. Rate the effects in terms of their severity (S).

8. Identify all of the potential (root) causes of each failure. This may also involve some brainstorming and refining.

9. Gather data on probability of occurrence and likelihood of detection of each failure mode. This may involve extensive research, testing, modeling, simulation, fault tree analysis, and other investigations.
10. Rate each failure mode's probability of occurrence (O). In cases where these ratings are disputed among team members or are otherwise uncertain, using the highest rating conceivable is the preferred approach.

11. Identify the existing means of detecting the failure and the actions that the system can take to prevent the ultimate effect from happening.

12. Rate the effectiveness (D) of the detection and mitigation currently available.

13. Calculate the Risk Priority Number (RPN) of each failure mode as the product of the S, O, and D values. In some cases, a sensitivity analysis may be warranted to determine sensitivity of the RPN to uncertainty in the factors S, O, and D.

14. Summarize initial findings and highlight critical failure modes or those which warrant further mitigation, based on the RPN (which indicates the overall criticality of the failure mode).

15. Assign responsibility to personnel (individual and/or subcommittee) for mitigation or elimination of failure mode. This usually results in suggested changes in the specification.

16. Revise FMECA form to reflect change in system resulting from corrective action. Ensure that team accounts for all effects on system and potential new failure modes resulting from the change.

17. Repeat process until RPNs are reduced to acceptable values.
APPENDIX II
FMECA Criteria
for Severity, Occurrence, and Detection
for ECP Cable Based Brake System Specifications
Revised January 29, 1999

Effect of Failure and Severity

Ask what happens if the failure occurs. The effect may be local to a particular device or car. The failure may impact other cars, the system as a whole, the mission (the scheduled trip), the surroundings (people and property near the train path). What is the worst possible ultimate effect? The severity of an effect of a failure should concentrate on the worst effect of the failure mode.

Severity Evaluation Criteria - the A S A value

<table>
<thead>
<tr>
<th>Effect</th>
<th>Rank</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>1</td>
<td>No effect. No train delays.</td>
</tr>
<tr>
<td>Slight</td>
<td>3</td>
<td>Slight effect on product or system performance. Short (&lt;10 min) train delay. Customer slightly annoyed. Personnel have discomfort</td>
</tr>
<tr>
<td>Minor</td>
<td>4</td>
<td>Minor effect on product or system performance. Train delay &lt; 1 hr. Customer experiences minor nuisance. Possible service stop. Personnel feels minor injury, can continue to work</td>
</tr>
<tr>
<td>Moderate</td>
<td>5</td>
<td>Moderate effect on product or system performance. Train delay for an hour. Customer experiences some dissatisfaction. Personnel hurt, hour lost from work</td>
</tr>
<tr>
<td>Extreme</td>
<td>8</td>
<td>Product inoperable but safe. System inoperable. Train stalled on track, can not be moved. Customer very dissatisfied. Personnel injured, weeks lost from work</td>
</tr>
<tr>
<td>Serious</td>
<td>9</td>
<td>Potential hazardous effect. Safety related - time dependent failure. Compliance with government regulation is in jeopardy. Possible runaway, collision, train derail and/or personnel disabled.</td>
</tr>
<tr>
<td>Hazardous</td>
<td>10</td>
<td>Hazardous effect. Safety related - sudden failure. Noncompliance with government regulation. Possible runaway, collision, train derail and/or person or people killed and/or severely disabled</td>
</tr>
</tbody>
</table>

* See Resolution of disagreement in ranking value below Occurrence table.
Causes of Failure and (rate of) Occurrence of those causes

We should list the root cause, not the symptom of the failure. First we are asking, *In what way can this system fail to perform as desired?*. Upon getting an initial answer, we should then ask *why* repeatedly until we get to the root cause. Causes can result from interaction of components with each other, interaction of the locomotive engineer, yard personnel, or others with the system, environmental, wear, software errors, intermittent contact, leakage, breakage, etc.

Occurrence Evaluation Criteria - the A O A value

<table>
<thead>
<tr>
<th>Occurrence</th>
<th>Rank*</th>
<th>Criteria</th>
<th>Average train miles to failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost Never</td>
<td>1</td>
<td>Failures unlikely</td>
<td>5,000,000</td>
</tr>
<tr>
<td>Remote</td>
<td>2</td>
<td>Rare number of failures likely</td>
<td>2,000,000</td>
</tr>
<tr>
<td>Very slight</td>
<td>3</td>
<td>Very few failures likely</td>
<td>750,000</td>
</tr>
<tr>
<td>Slight</td>
<td>4</td>
<td>Few failures likely</td>
<td>290,000</td>
</tr>
<tr>
<td>Low</td>
<td>5</td>
<td>Occasional number of failures likely</td>
<td>130,000</td>
</tr>
<tr>
<td>Medium</td>
<td>6</td>
<td>Medium number of failures likely</td>
<td>45,000</td>
</tr>
<tr>
<td>Moderately high</td>
<td>7</td>
<td>Moderately high number of failures likely</td>
<td>17,000</td>
</tr>
<tr>
<td>High</td>
<td>8</td>
<td>High number of failures likely</td>
<td>7,000</td>
</tr>
<tr>
<td>Very high</td>
<td>9</td>
<td>Very high number of failures likely</td>
<td>2,500</td>
</tr>
<tr>
<td>Almost certain</td>
<td>10</td>
<td>Failure almost certain</td>
<td>1,000</td>
</tr>
</tbody>
</table>

*Resolution of disagreement in ranking value:*

If the numerical value falls between two numbers, always select the higher number.

A process to use:

1. If the disagreement is an adjacent category, average out the difference. For example, if one member says 5 and someone else says 6, the ranking average is 5.5, so assign it to 6.

2. If the disagreement jumps one category, then consensus must be reached. Even with one person holding out total consensus must be reached. No average, no majority. Everyone in that team must have ownership of the ranking. They may not agree 100 percent, but they can live with it.
Detection Method and counter-measures

Describe what method is being used to detect the cause of the failure and the actions being taken by the various parts of the system to counter or mitigate the potential problems of the failure. If there are none, then the column should so indicate. What sub-system parts are involved - electronic, pneumatic, mechanical, visual and audible warnings, human interaction/intervention?

Detection Evaluation Criteria - the A D A value

Detection is a rating corresponding to the likelihood that the proposed system controls will detect and mitigate a specific root cause of failure. If the ability of the controls to detect the failures is unknown, then the rating should be 10. Consideration should be given to reliability of the parts of the sub-system involved in the detection and counter-measures.

<table>
<thead>
<tr>
<th>Detection</th>
<th>Rank*</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost certain</td>
<td>1</td>
<td>Has the highest effectiveness in each applicable category</td>
</tr>
<tr>
<td>Very high</td>
<td>2</td>
<td>Has very high effectiveness</td>
</tr>
<tr>
<td>High</td>
<td>3</td>
<td>Has high effectiveness</td>
</tr>
<tr>
<td>Moderately high</td>
<td>4</td>
<td>Has moderately high effectiveness</td>
</tr>
<tr>
<td>Medium</td>
<td>5</td>
<td>Has medium effectiveness</td>
</tr>
<tr>
<td>Low</td>
<td>6</td>
<td>Has low effectiveness</td>
</tr>
<tr>
<td>Slight</td>
<td>7</td>
<td>Has very low effectiveness</td>
</tr>
<tr>
<td>Very Slight</td>
<td>8</td>
<td>Has lowest effectiveness in each applicable category</td>
</tr>
<tr>
<td>Remote</td>
<td>9</td>
<td>Is unproven, or unreliable, or effectiveness is unknown</td>
</tr>
<tr>
<td>Almost impossible</td>
<td>10</td>
<td>No technique available or known, and/or none is planned.</td>
</tr>
</tbody>
</table>

* See Resolution of disagreement in ranking value below Occurrence table.

RPN: Risk Priority Number

The RPN value is the product of Severity, Occurrence, and Detection. The RPN value is used only to rank the potential system deficiencies. A higher number generally indicates that more attention should be paid to the cause to reduce its likelihood or find ways to mitigate the effects.
# APPENDIX III
## Definitions of Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCP</td>
<td>Brake Cylinder Pressure</td>
</tr>
<tr>
<td>CCD</td>
<td>Car Control Device</td>
</tr>
<tr>
<td>D rating</td>
<td>Detection</td>
</tr>
<tr>
<td>ECP</td>
<td>Electronically Controlled Pneumatic</td>
</tr>
<tr>
<td>ECPB</td>
<td>Electronically Controlled Pneumatic Brake</td>
</tr>
<tr>
<td>EOT</td>
<td>End of Train Device</td>
</tr>
<tr>
<td>FMEA</td>
<td>Failure Modes and Effects Analysis</td>
</tr>
<tr>
<td>FMECA</td>
<td>Failure Modes, Effects, and Criticality Analysis</td>
</tr>
<tr>
<td>FTA</td>
<td>Fault Tree Analysis</td>
</tr>
<tr>
<td>HEU</td>
<td>Head End Unit</td>
</tr>
<tr>
<td>mfr.</td>
<td>Manufacturer</td>
</tr>
<tr>
<td>O rating</td>
<td>Occurrence</td>
</tr>
<tr>
<td>PB</td>
<td>Pneumatic Backup</td>
</tr>
<tr>
<td>RPN</td>
<td>Risk Priority Number</td>
</tr>
<tr>
<td>S rating</td>
<td>Severity</td>
</tr>
<tr>
<td>spec.</td>
<td>Specification</td>
</tr>
<tr>
<td>TL</td>
<td>Train Line</td>
</tr>
</tbody>
</table>
APPENDIX IV
FMECA for Specification S-4200 (April 1, 1999)

Part B File: FMECA of S-4200 1999 07 19 4_4.xls Pages IV-B-1 thru 142