A. Purpose

This Manual Part recommends the application design guidelines for isolation of power supplies external to used with vital signal equipment.

B. General

The vital circuit design guidelines provided in this manual part represents one type of circuit design for providing power supplies for signal circuitry. Some aspects of the circuit design may vary depending on the design practices of individual railroads.

C. Design

1. It is extremely important that dc power supplied for vital circuits is isolated from the power supplied to non-vital parts of the signal system not meeting Manual Parts 15.2.5 Recommended Dielectric Requirements for the Design and Installation of Electrical Equipment and Other Electrical Devices and 11.5.1 Recommended Environmental Requirements for Electrical and Electronic Railroad Signal Equipment. A surface leakage distance of not less than 1/4 in (6.35 mm) shall be provided between any exposed metallic part of the apparatus carrying current and any other metallic part hereof. This approach to design is needed to prevent grounds on non-vital equipment from creating a potential unsafe failure of the vital circuitry.

Some communication systems (specifically radio-based communications) require the dc power system to be earth-grounded. The potential for failure also exists when wire insulation breaks down on a non-vital circuit allowing that circuit to become grounded. In the first case the ground is known but in the second case the ground is unknown. In either case, a second failure on a vital circuit wire could bypass some of the required vital logic if isolation is not applied.

Figure 1632-1 shows an example of how a ground can bypass critical safety logic in a vital signal repeater circuit. It can easily apply to any vital circuit.
2. The following two methods of isolation are recommended to separate vital and non-vital dc power:
   a. Independent battery banks and chargers for vital and non-vital circuits.
   b. Use of a dc/dc converter with an input to output isolation rating of either 2000 Vrms for electronic circuits or 3000 Vrms for relay logic circuit applications as per Manual Part 11.5.1.

3. It is recommended that periodic maintenance testing be performed to determine that there are no grounds or isolation faults on all power supplies that feed vital circuitry.
A. Purpose

This Manual Part recommends vital circuit design guidelines for time locking applications at interlockings and control points.

B. General

1. Time locking is required to prevent an established route from being changed until a predetermined time interval has elapsed. Time locking is initiated when a signal has been set to stop by means other than normal train operation.

2. The vital circuit design guidelines provided in this Manual Part shall also apply to equivalent vital software applications.

3. The vital circuit design guidelines provided in this Manual Part represent one method of design for time locking applications. Some aspects of the circuit design may vary, depending on the design practices of the individual railroad.

C. Design

1. An example of time locking is shown in Figure 1641-1. When the route aligns in agreement with the request, the Route Check Relay (1WRCSR) becomes energized which de-energizes the Approach Stick Relay (1WASR). The de-energized 1WASR prevents a change of any switch position in the established route and prevents clearing a signal for any conflicting route. When the signal clears, the Red Signal Repeater Relay (1WRGPR) de-energizes which prevents the initiation of a time release or a track release of the 1WASR until the signal is set to stop and the 1WRGPR re-energizes.

Time release of the 1WASR is initiated over the back contact of the 1WASR when the 1W signal is set to stop. When the preset time for the Time Element Relay (1WASTER) elapses, the 1WASTER energizes permitting the 1WASR to become energized over the front contact of the 1WASTER. When the 1WASR energizes, battery is removed from the 1WASTER. The stick circuit maintains the 1WASR when the 1WASTER de-energizes. The time setting of the 1WASTER shall conform to Manual Part 2.4.20 Recommended Instructions for Time Releases Applied to Signal Apparatus. The front contact of the Track Relay (9TR) prevents
unnecessary operation of the timer once the train passes the signal. This contact is only used when the track release is also used.
The track release is used when it is desirable to release the locking by re-energizing the 1WASR as soon as possible to establish another train movement. Two track release 9TPR and 5TPR or 9TPR and 7TPR track repeater relays, as opposed to single track release, is recommended as shown to prevent an inadvertent, momentary de-energizing of the track relay from releasing the locking. The Normal and Reverse Switch correspondence Relays (7NWCR and 7RWCR) provide selection of the track release contacts in accordance with the established route.

Equivalent Boolean expressions for the 1WASR and 1WASTER control circuits shown in Figure 1641-1 are as follows:

\[
(1\text{WASR}) = \overline{(1\text{WRCSR})} \times (1\text{WRGPR}) \times ((1\text{WASTER}) \\
+ (1\text{WASR}) \\
\quad + (9\text{TPR} \times ((5\text{TPR} \times 7\text{NWCR}) \\
\quad \quad + (7\text{TPR} \times 7\text{RWCR})) \times \text{POSR}))
\]

\[
(1\text{WASTER}) = \overline{(1\text{WRCR})} \times (1\text{WRGPR}) \times \overline{(1\text{WASR})} \times 9\text{TR}
\]

2. In processor-based systems, application logic shall be provided to require time-locking to run upon initialization of the system. Time locking may be cancelled when system logic determines no trains are approaching.

3. In systems using ac track circuits, a Power-Off Stick Relay (POSR) is required to prevent a false release of locking for an established route following a momentary power outage and subsequent restoration of power. This prevents the dropping of all of the track circuits from re-picking the ASR relay.

4. In systems without standby power, a Power-Off Stick Relay (POSR) is also required to prevent a false release of locking for an established route following a momentary power outage and subsequent restoration of power.

For example, when a momentary ac power outage occurs, all relays will de-energize. When power is restored, all relays in the pickup circuit of the 1WASR will energize immediately; however, the track relays may energize slower allowing the 1WASR to pick up which would falsely release the locking.

The POSR circuit can prevent this false release by forcing time to run before the 1WASR is allowed to pick up. The POSR is controlled through front contacts of the Power-Off Relay (POR) and the 1WASR. A front contact of the POSR is placed in the pick-pick-up circuit of the 1WASR. When power
is restored, the POSR open front contact will prevent the 1WASR from energizing and will force time to start running. With the POR energized and when the 1WASR is energized, after time has expired, the POSR will be permitted to reset. A stick circuit is provided to bypass all ASR contacts for normal operation.

Equivalent Boolean expression for the POSR control circuit shown in Figure 1641-1 is:

\[
\text{POSR} = \text{POR} \times (\text{POSR} + (1\text{EASR} \times 1\text{WASR} \times 1\text{EASR} \times 2\text{EASR} \times 2\text{WASR} \times 3\text{EASR}))
\]

At interlockings where signals may be fleeted, the POSR circuit shown in Figure 1641-1 will not function. When any of the signals are fleeted, the corresponding ASR remains de-energized. When the power fails and resumes, the POSR remains de-energized. To prevent this, the circuit shown in Figure 1641-2 may be utilized. Here, the POSR operation is independent of the ASR and fleeting has no effect on the POSR. In the event of power failure with all signals at stop, the ASR contacts eliminate the need to run time.

Equivalent Boolean expression for the POSR and POTER control circuits shown in Figure 1641-2 are as follows:

\[
\text{POSR} = \text{POR} \times (\text{POSR} + (\text{POTER} + (1\text{EASR} \times 1\text{WASR} \times 1\text{EASR} \times 2\text{EASR} \times 2\text{WASR} \times 3\text{EASR})))
\]

\[
\text{POTER} = /\text{POSR} \times \text{POR}
\]

5. When a common timer is used, such as the 1WASTER shown in Figure 1641-1, which in this example would be common for the 1W and 1WD signals, the actual time setting shall be the maximum time release required for the 1W or 1WD signal. If there is a considerable difference in the time requirements, separate timers may be required. Whenever common timers are used, precautions shall be taken to prevent a premature release of locking caused by the release of any conflicting ASR.

6. The check contact of electro-mechanical type timers shall be checked in the signal network to ensure the timers have reset to their zero time position when energy is removed from the timers.
Figure 1641-1: Time Locking and Power-Off Stick Circuits
Figure 1641-2: Power-Off Stick Circuit Where Signals May Be Fleeted
A. **Purpose**

This Manual Part recommends vital circuit design guidelines for loss-of-shunt circuits.

B. **General**

1. This Manual Part presents design guidelines and methodologies for prevention of improper operation of vital circuits in the event of a momentary loss of shunt.

2. These vital circuit design guidelines also apply to equivalent vital software applications.

3. The vital circuit design guidelines presented in this Manual Part represent several methods of design of loss-of-shunt circuits. Some aspects of the designs may vary depending on the design practices of the individual railroad.

C. **Loss of Shunt**

Track circuits are used within signal control systems to detect track occupancy when the track circuit is shunted by a train. Signal control circuits are selected through the output of track relays or devices that function as track relays. Loss of shunt can occur because of rusty rail, presence of foreign matter, and other adverse conditions.

D. **Circuit Design**

1. The circuit design shall ensure that a loss of shunt of five seconds or less shall not permit an established route to be changed or released.

2. Figures 1648-1 through 1648-3 illustrate various methods of negating the effects of a momentary loss of shunt. In each of the three circuits, a delay is introduced into the response time of the track circuit by employing vital timing devices and track repeater relays. In circuits where electromechanical timing devices are used, a check contact of the timing device may be available to verify that the timing device is ready for operation and not running time. In all cases, a loss of shunt of five seconds or less shall not permit the track repeater relay to re-energize. Actual operating time of the timing device may
be increased depending on local or system operating criteria or standards. The output of the track repeater relay then is used in the control of the vital circuits at interlockings and control points.

**Figure 1648-1: Loss-of-Shunt Circuit Using Time Element Relay**

a. Figure 1648-1 is an example of a loss-of-shunt circuit implemented with a time element relay. When no trains are present, track repeater relay 1TPR is energized through its own contacts and the contacts of the track relay, 1TR. When the track circuit is shunted, the contacts of 1TR open, thus releasing 1TPR. The entire circuit remains de-energized until the shunt is removed. When that happens, energy is first applied to the coil of the time element relay, 1TTER, through contacts of 1TPR and 1TR. Note however, that 1TPR cannot be re-energized until the contacts of 1TTER are closed.
1TTER will not re-energize until the preset time interval of five or more seconds has elapsed. If the track circuit is shunted before the time interval is complete, 1TR will release, energy will be removed from the circuit, and 1TTER will be reset. Hence, 1TPR will remain released-de-energized if the shunt is removed for any period of time less than the preset interval of 1TTER. Once 1TTER is re-energized for the full interval, 1TPR is energized through contacts of 1TTER and 1TR. Subsequently, 1TTER is released and 1TPR remains energized through the transfer of contacts of 1TPR. The circuit is then ready to perform another complete cycle.
The equivalent Boolean expressions for the loss-of-shunt circuit shown in Figure 1648-1 are as follows:

\[ 1TPR = 1TR \times (1TTER + 1TPR) \]

\[ 1TTER = 1TR \times \overline{1TPR} \]

b. A loss-of-shunt circuit using a thermal relay is shown in Figure 1648-2. Because of the operating characteristics of thermal relays, it is recommended that this type of circuit only be used in low-density traffic territory. When the track circuit is shunted, track relay 2TR is released. When 2TR contacts open, track repeater relay 2TPR is released. When the shunt is removed, the heating coil of 2THER is heated as a result of the current flow through the low resistance path from B to N through the contacts of 2TR and 2TPR. As the heating coil of 2THER heats up over time, the bi-metallic strip of 2THER causes its contacts to close, thereby re-energizing 2TPR. 2TPR is then held energized through its own contacts, the
heating coil of 2THER and the contacts of 2TR. The addition of the coil of 2TPR into the circuit increases the overall series resistance and current flow is reduced, the heating coil of 2THER cools, and the contacts of 2THER are opened. It is the slow response of the bi-metallic strip of 2THER that prevents 2TPR from responding to a momentary shunt loss.

Figure 1648-3: Loss-of-Shunt Circuit Using Solid State Timing Device

c. A solid state timing device is used in the loss-of-shunt circuit of Figure 1648-3. This type of timer provides a momentary output pulse after a continuous input is present for a predetermined time interval. When the track is shunted, the contacts of 3TR open and remove energy from the timer input and the contacts of 3TPR. No voltage is present at the output of the solid state timer, thus 3TPR is released. When the shunt is removed, continuous input must be maintained for a preset
interval before the solid state timer will produce a momentary output pulse. Each time energy is removed, the timer is reset. Once the preset interval requirements are met, a momentary pulse appears at the output of the timer and 3TPR is energized. Once energized, 3TPR is held through its own contacts. Subsequently, the output of the solid state timer is removed and the loss-of-shunt circuit is ready for the next operation.

The equivalent Boolean expressions for the loss-of-shunt circuit shown in Figure 1648-3 are as follows:

\[ 3TPR = 3TR \cdot (3TPR + 3TE) \]
\[ 3TE = 3TR \]

d. Loss-of-shunt timing function may be implemented in vital application software of processor-based systems by assigning a pick-up delay to a track circuit input.
A. **Purpose**

This Manual Part recommends vital circuit design guidelines for spring switches.

B. **General**

1. The vital circuit design guidelines recommended in this Manual Part apply to spring switches.

2. The objective of these guidelines is to describe the vital circuit design criteria for switch point detection at spring switches in general, with additional consideration given to spring switch installations having a higher potential of damaged or bent switch point detector rods due to ice build up in the switch crib bed.

3. The vital circuit design guidelines provided in this Manual Part shall also apply to equivalent safety critical software applications.

4. The vital circuit design guidelines provided in this Manual Part represent one method of design for spring switch circuits. Some aspects of the design may vary depending on the design practices of the individual railroad.

C. **Spring Switch Operation**

1. A spring switch is a term used to describe a switch equipped with a mechanical buffer or spring mechanism. The spring mechanism is attached to the throw rod of a hand throw switch stand.

2. Spring switches are typically installed at the ends of passing sidings or junctions with the main track. They provide for more efficient train operation by eliminating the need for train crews to stop and manually operate a hand throw switch (normal to reverse) when exiting a siding.

3. Switches are typically left lined for the predominant route (normal). When hand throw switches are used, train crews may be required to manually operate the switch for both facing point and trailing point movements over the switch reverse. The spring switch however is designed to return the points of a switch back to their original position.
after being forced open (compressing the spring) by the first wheels of a train, as it passes over the switch during a trailing movement. As each set of wheels of the train passes though the switch points, they are maintained in the reverse by the hydraulic buffering feature of the spring switch mechanism that prevents the coiled spring from fully de-compressing instantly. It normally takes approximately 10 to 12 seconds for the switch points to return to the full normal position. This reduces the potential of excessive wear on the switch points and spring switch mechanism.

Note: Train movements entering into a siding (facing point movements) equipped with a spring switch must always stop, reverse the switch manually, complete the entire movement and then return the switch to the normal position.

D. Circuit Design

1. The position of the switch points on a spring switch are checked in the same manner as that of a hand throw switch by attaching a detector rod from the point to a switch circuit controller (SCC). The SCC is then adjusted to detect the normal position of the switch points. Contacts of the SCC are inserted into either the track circuit or the signal control line circuit, depending on the design of the system. If the switch points remain reverse or do not return to the normal position, the circuit design will prevent a main track signal clearing into the section of track where the spring switch is located. Refer to Figure 1664-1. On some railroad’s, spring switch point detection is not checked by signals governing trailing point moves over the switch.

2. The SCC circuits shown in Figure 1664-1 illustrate the use of what is commonly referred to as "break and shunt" circuits. The normal contacts (N) of the SCC are designed to open the control circuit of the track relay or signal control line relay when the switch point moves 1/4 in (6.35 mm) or more from the normal position. The reverse contacts of the SCC then shunt the relay side of the circuit.

3. Spring switch point detection circuits also may employ what is referred to as "frozen rod detection" in territories where extremely cold weather conditions may sometimes result in a high ratio of broken point detector rods. The point detector rod is subjected to much higher forces than that of a hand throw switch because of the trailing feature of the switch and the fact that the train wheels force the points reverse. Where climatic conditions are such that the point...
detector rod becomes frozen in place due to ice buildup in the switch crib, causing the rod to bend or sometimes break because of the stresses applied by the train wheel, it is necessary to provide another level of switch point detection.

4. Frozen rod protection is a term used to describe the SCC circuits shown in Figure 1664-1, which demonstrate the application of two SCCs: one which is used on the point detector rod (PD-X) and the other which is used to detect the position of the throw rod (T-X). The break and shunt contacts of both SCC’s are in series with the SSOSTR (spring switch on station track relay).

Without the additional SCC on the throw rod, the circuits may not be able to properly detect the actual position of the switch points. If the point detector rod was to break and remained frozen in the crib bed, and the circuits may falsely indicate the switch points are actually in the normal position. The additional SCC on the throw rod provides a redundant check on the actual position of the switch points by detecting the corresponding position of the throw rod.

As shown in Figure 1664-1, the SSOST will remain de-energized if either the T-X normal or PD-X normal contacts remain open or their respective reverse contacts remain closed.

![Figure 1664-1: Spring Switch SCC Circuits](image-url)
A. **Purpose**

This Manual Part recommends the vital circuit design guidelines for slide fences.

B. **General**

1. The vital circuit design guidelines provided in this Manual Part shall also apply to equivalent vital software applications.

2. The vital circuit design guidelines provided in this Manual Part represent one type of circuit design for providing the slide protection for signalled train movements. Some aspects of the circuit design may vary depending on the design practices of individual railroads.

C. **Design**

1. In specific types of terrain it may be necessary to guard against the possibility of derailments from land, snow or ice slides. Detection of a significant slide will be used to inform approaching trains that the track infrastructure has changed or an obstruction may be blocking the track ahead. Detection of a slide can be accomplished in a number of ways. The most common approach is to use a detection fence that parallels the tracks.

   Activation of the slide fence shall give a restrictive indication to all approaching trains. Figure 1691-1 shows an example of a section, AX-BX, of track that is vulnerable to slides.

2. Slide fence designs are tailored to different terrain. The different types of terrain are:

   **Rock Cuts:** They can vary depending upon how steep the slope and how close the cut is to the track. When the cut is close to the track and fairly vertical, then overhead sections of the slide fence are required to detect falling material that could miss the vertical fence.

   **Potential bank slides of mud and rock:** This type can be detected with the conventional fence or with tilt measuring devices to determine movement.

   **Slopes that accumulate ice or snow:** This type can be detected with the conventional fence with or without overhead sections.
3. Two examples of designs that may be used are as shown in Figure 1691-1 and 2 but are only different in the way in which they activate the warning system.

   a. Example 1: Movement detected by the slide fence is transmitted through an operating pipe and trigger arrangement that unlatches a spring to operate a circuit controller. The controller is usually mounted on a mast between each slide fence section. The slide fence is loosely stapled to all intermediate slide fence posts to allow lateral movement.

   b. Example 2: Slides are detected by the fence by breaking the physical wires that run the full length of the fence. The wires are stapled or permanently connected to the poles as shown in Figure 1691-2 and are separated from one another by about 8 inches (203 mm) to allow small rocks or ice to fall through without wire breakage. To protect against bypassing a section of the fence when a wire breaks, consideration should be given in the circuit design to provide a manual reset.

4. Warning to approaching trains can be offered in the following methods:

   a. A special signal can be erected to advise whether a slide has or has not been detected. This shall be used in areas where there are no signals, and may be used in addition to conventional signals.

   b. If the slide fence is located in signal territory the controller contacts in the normal position or the contacts of the slide fence relay shall be included in the signal control circuits in such a way they will open the circuit in the event a slide is detected. In certain TCS applications, circuits may be arranged so that only the signals governing movement through the slide area display restrictive aspects as opposed to generating a full tumble down.

   c. As an alternative to 4.a above, or in addition to 4.b above, movement may continue through the area if a voice radio message is received indicating the absence of a slide.

   d. Some defect detecting systems report exceptions only. These systems shall report system health via another means.
Figure 1691-1 Using Controllers Along the Fence
Figure 1691-2  Using Only a Wire Fence

NOTE: BOTTOM WIRE TO BE 36" FROM GROUND.

* DENOTES COPPER WIRE
** DENOTES ACSR
A. Purpose

This Manual Part recommends a safety assurance program for electronic/software based products used in safety-critical (vital) applications, that is designed to ensure their safety throughout their life cycle.

B. General

1. The safety assurance program described in this Manual Part should be considered a guideline to manufacturers and railroads involved in the development, manufacturing and utilization of electronic/software based products used in safety-critical (vital) applications.

These guidelines exclude end-user developed application software (e.g. interlocking Boolean equations).

The following Manual Parts provide additional detail related to a safety assurance program.


2. The safety assurance program described in this Manual Part should support the achievement of applicable requirements of subparts H and I of 49 CFR Part 236, for Processor-Based Signal and Train Control Systems and Positive Train Control Systems, respectively.

3. Top level safety goals include:

   a. The product shall operate safely under normal operating conditions.

   b. The product shall operate safely under adverse operating conditions (environmental, operating stress).
c. The product shall operate safely, or maintain a safe state, under all credible failure conditions.

4. A fundamental requirement for electronic/software-based products used in safety-critical (vital) applications and systems is that the design requirements shall be validated and the operation shall be verified for safety prior to acceptance.

C. **Product Design Considerations**

1. Product design should take into account expected use and reasonably foreseeable misuse of the equipment to mitigate hazards.

2. Product design should consider the safety of installer, maintainer and user.

3. Product design should consider the applicable portions of established industry practices or standards as promulgated through appropriate standard-making bodies. These standards include:
   
   
   
   
   
   
4. Provisions should be made for periodic functional checks of safety devices and features incorporated into the product.

5. Warning and caution notes should be provided in installation, maintenance, and repair instructions.

6. Distinctive warning markings should be provided on any hazardous components that may affect personnel safety.

7. The product shall conform to the environmental limits of Manual Part 11.5.1 Recommended Environmental Requirements for Electrical and Electronic Signal Systems. Consideration should be given to ensuring that the product does not fail in an unsafe manner when these limits are exceeded.

8. Adjustable components should be located so that exposure to hazards by installation, maintenance and operating personnel is minimized.

9. Ergonomic engineering (user-friendly) factors should be taken into account in the design of the product.


11. Design shall make reasonable provisions to mitigate unsafe failures arising from procedural error, neglect, and vandalism.

12. Product design shall be such that failures that cause unacceptable or undesirable hazards are eliminated by design. Failures that are non-self-revealing shall not cause unacceptable or undesirable hazards, even in combination with subsequent failures.

For signal and train control applications, the safe state is defined as causing a more restrictive aspect to be displayed, trains to stop, a speed limit known to be safe to be imposed, or a specific sequence of operations known to be safe to be followed.

13. Provisions shall be made to ensure that common-cause failures do not result in an unsafe condition.

14. Electronic/software based products purchased from a third party, which have an effect on safety, are subject to the safety considerations discussed in this Manual Part. The analysis can either be provided by the third party (in line with these recommended practices) or performed by the purchaser.
15. The following characteristics of processor-based systems are widely accepted as necessary to achieve systems that provide a level of safety at least as great as previous generation systems. Deviation from these characteristics needs to be specifically addressed in a safety analysis. Further information on these attributes can be found in:


a. Simplicity is a critical aspect for any safety-critical design. Simplicity allows a more complete understanding of the system operation minimizing the chances for error. Simplicity also minimizes the number of interfaces with other systems, making the designs easier to test and reducing another common source of error. Drastically reducing the number of functions performed by the safety-critical system (and enforcing this reduction) also keeps function creep under control and allows future changes to be made and verified.

Complex software systems are easier to build than simple ones. (e.g. For example, use of an operating system makes the design simpler but adds complexity, thereby making it more difficult to be analyzed. If an operating system is used, the safety analysis must identify how safety is not affected.)

b. Deterministic software is a major advantage in processor-based systems used for safety-critical applications. Since communication among all the components is known at design time, the system can be designed without the need for complex inter-process communications that would normally be provided by an operating system or dynamic memory management. Leveson identifies four underlying requirements for deterministic systems:

- First, there is a need for strict time controls. Many of the required functions need to be repeated on a periodic basis.

- Secondly, there is a need for analyzing algorithm behavior with the ability to consistently predict how it will behave in the future.

- Thirdly, an ability to test software and obtain consistently repeatable results (e.g. not dependent on random timing) is
needed.

- Finally, deterministic behavior is necessary to provide the human interface in such a way that the displayed information is consistent in a variety of situations. This need for deterministic operation highlights that a simple, deterministic system can be more difficult to design and develop than a complex system.

c. Separation of safety-critical functions from the non-safety-critical functions is an essential characteristic of safety-critical systems. This reduces the complexity and coupling of the safety-critical system allowing it to be implemented with a much higher degree of confidence. In addition, the separation allows the safety analysis to be performed on a manageable portion of the system. The complexity of a system grows exponentially as the number of its functions increase. In such cases, separation of safety-critical from non safety-critical functions becomes more critical in order to achieve practical systems.

d. Decoupling is another attribute desirable in developing a safety-critical design. This ensures that one component will not affect the operation of another component. Tightly coupled systems substantially increase the risk of faults due to unintended interrelationships between components. Once again, tightly coupled systems are typically more efficient and require less design effort than loosely coupled systems. However, the interdependence of these tightly coupled components adds new hazards to the safety-critical system.

16. The product design shall require positive actions to be taken in a prescribed manner to either begin its operation or continue its operation (closed loop principle).

D. Safety Assurance Program

1. The objective of a Safety Assurance Program is to provide proof-of-safety of electronic/software-based products being developed for safety-critical (vital) applications. An integrated approach should be followed to meet this objective.

2. The integrated approach should consist of three programs:

a. Quality Management
b. Safety Management

c. Safety Verification & Validation (V&V)

3. Quality Management

A Quality System conforming to Manual Part 17.2.1 Recommended Quality Assurance Program for Electronic/Software-Based Products Used in Vital Signal Applications should be followed.

4. Safety Management

A safety management program should be in place throughout the life cycle of electronic/software-based products used in safety-critical (vital) applications. This program should consist of the following steps, in the order listed:

a. Safety Organization

(1) A safety organization should be in place or set up prior to the start of the development of the equipment or system.

(2) The objective of the safety organization is to manage the overall safety assurance program.

(3) The safety organization should preferably be independent of the design function and should have the ability to determine the completeness and correctness of the safety activities.

(4) The final release of a new vital system should require the approval of the safety organization.

(5) An effective safety organization should clearly identify its management structure, and specific responsibilities and roles of the safety assurance personnel within the organization.

b. Safety Program Plan

(1) The objective of the Safety Program Plan is to provide a structured approach to planning and implementing the safety assurance program. It should identify the safety organization, safety assurance activities, and safety-related documentation needs of the system under consideration.
(2) A V&V Plan should be an integral part of the Safety Program Plan.

c. Preliminary Hazard List

(1) A Preliminary Hazard List (PHL) should be compiled very early in the equipment/system acquisition life cycle to identify potentially hazardous areas on which to put management emphasis.

(2) Safety experience on similar equipment/systems, including mishap/incident hazard tracking logs if available, safety lessons learned, etc., should be used in preparing the PHL.


d. Preliminary Hazard Analysis

(1) The Preliminary Hazard Analysis (PHA) should be conducted during the early stages of the development.

(2) The objective of the PHA is to analyze the potential hazards from the PHL and other sources, and the associated risks so that safety concerns can be addressed early and the design can be appropriately directed.

(3) A Hazard Log should be used as a reference to track the resolution of the identified hazards as the system development progresses.

(4) See Manual Part 17.3.5 for additional supporting information.

e. Product Safety Requirements

(1) The objective of this step is to identify the overall safety requirements for the product, based on the overall functional requirements, user requirements, and safety concerns of electronic/software-based products in general.
(2) The PHA should be used as a guide in preparing the Product Safety Requirements (PSR). The PSR should be revised as new hazards are identified and the detailed hazard analyses are performed.

f. Safety Requirements Allocation

The objective of this step is to allocate the safety requirements to hardware and software; based upon the PSR and architectural design decisions, including the overall safety design philosophy that is being followed for the product.

g. Detailed Hazard Analyses

(1) Detailed hazard analyses such as Subsystem Hazard Analysis (SSHA), System Hazard Analysis (SHA), Operating & Support Hazard Analysis (O&SHA), Fault Tree Analyses (FTA), Functional Fault Trees (FFT) and Failure Modes and Effects Analysis (FMEA) should be conducted on the product as the design progresses.

(2) The objective of these analyses is to help identify various hazards and their associated risks, and the possible means of eliminating the hazards or reducing their risks to acceptable levels. The analyses also help identify the V&V requirements and provide a measure of the completeness of the V&V activities.

h. Safety Verification & Validation

The objective of this key element of the Safety Management program is to demonstrate compliance with all safety requirements and to provide a final proof-of-safety of the product. Refer to Section E below.

i. Safety Assurance During the Lifecycle

During the lifecycle of the product, the Safety Management process shall ensure that safety is not affected by hardware, software and other product-related modifications subsequent to release of the product.

j. Safety and Design Reviews
(1) In addition to the preceding steps, safety reviews should be an integral part of design reviews and of the Safety Management process. Results of qualitative and quantitative assessment of the design should be reviewed and recorded to determine if the established safety allocation goals have been achieved. Safety reviews should be conducted throughout the product lifecycle.

(2) The objective is to ensure that critical safety activities are carried out at their appropriate times, and that safety issues are resolved in a timely manner.

(3) The Hazard Log should be used to record and track the resolution of the hazards identified in the PHA, the detailed hazard analyses, and during the product lifecycle.

E. **Safety Verification & Validation**

1. The Safety Verification and Validation process is a key part of the Safety Management process and therefore has been addressed separately.

2. The objective of the Safety V&V activity is to verify and validate the safety requirements.

3. The Safety V&V process should consist of the following activities:

   - Safety V&V Planning
   - Product Safety Requirements Validation
   - Hardware Safety Verification and Validation
   - Software Safety Verification and Validation
   - Product Safety Validation (following Hardware/Software Integration)
   - Safety V&V of Modifications

The above Safety V&V activities and their relationship to a typical product development cycle are shown in Figure 1731-1 and are elaborated on below.

   a. Safety V&V Planning
In the early stages of the product development and as an integral part of the Safety Program Plan, the Safety V&V activities should be planned. A sub-plan should be prepared for each of the Safety V&V activities identified in Figure 1731-1.

b. Product Safety Requirements - Validation

This activity validates that the PSR accurately reflects all of the product safety requirements as dictated by the user and/or the intended application of the product. The PSR should be reviewed for correctness, completeness, unambiguity, and consistency, and should be done per a Product Safety Requirements Validation Plan.
c. Hardware Safety Verification and Validation

These activities should include:

(1) Hardware safety requirements allocation validation to ensure that the allocations accurately reflect the safety-critical and safety-related hardware requirements, that human error has not occurred, that there are no omissions or commissions, and that the allocations are complete, correct, unambiguous and properly mapped to the Product Safety Requirements specification. (Validation that hardware safety allocations are complete and correct.)

(2) Hardware design verification to demonstrate safe operation of the hardware under normal operating conditions as well as under single point and non-self-revealing fault conditions in hardware that does not rely on software for safety. (Verify that the design meets its safety requirements.)

(3) Hardware implementation verification to demonstrate that hardware implementation correctly and accurately reflects the hardware design. (Verify that the hardware is built as designed.)


d. Software Safety Verification and Validation

This activity should include:
(1) Software safety requirements allocation validation to ensure that the allocations accurately reflect the safety-critical and safety-related software requirements, that human error has not occurred, that there are no omissions or commissions, and that the allocations are complete, correct, unambiguous and properly map to the Product Safety Requirements specification. (Validation that software safety allocations are complete and correct.)

(2) Software design verification to demonstrate that the design (and design specifications) correctly reflects the safety requirements, and that human error has not occurred during the design process (design of incorrect safety-related function, failing to design a safety function, and/or designing a safety function incorrectly). (Verify that the design meets its safety requirements).

(3) Software code verification to demonstrate that the code correctly reflects the safety requirements and that human error has not occurred during the coding process (coding of incorrect safety-related function, failing to code a safety function, and/or coding a safety function incorrectly).

(4) Software module testing to demonstrate that each software module performs its intended safety function correctly and does not operate in an unsafe manner. (Verify that the software module is safe as designed.)

(5) Software integration testing to demonstrate that the software modules integrate correctly, by progressively combining the modules into a composite whole and verifying safe interaction between the modules.

e. Product Safety Verification and Validation

(1) An overall product safety verification and validation shall be conducted following the integration of all hardware and software, and after all separate hardware and software V&V activities have been completed. The purpose is to demonstrate compliance with the PSR and that the product is "fit for purpose" from a safety viewpoint.

(2) This activity includes a final product safety description, an overall V&V review, and a final hardware/software integration
verification. It should involve demonstrating the safety of hardware portions that were not addressed by the earlier hardware V&V activities. This should include the hardware that relies, at least in part, on software to ensure safe operation.

(3) This activity should also involve testing which demonstrates safe operation of the software and the overall product under normal input conditions (operational profiles), external influences (electrical, mechanical and climatic), and under various hardware fault conditions.

f. Safety V&V During the Life-Cycle of Modifications

A safety V&V program shall be provided to include review and V&V of each modification to the product during its lifecycle to ensure that the modifications to the original requirements, design, or implementation do not compromise safety.

F. Risk Assessment

AREMA® C&S Manual

Part 17.3.3

Recommended Practice for Hardware Analysis for Vital Electronic/Software-Based Equipment Used in Safety-Critical (Vital) Applications

Revised 2007-20176 (24116 Pages)

A. Purpose

This Manual Part recommends hardware analysis requirements to be used as part of the analysis of vital electronic/software based equipment and systems used in safety-critical (vital) applications.

B. General

1. This Manual Part contains a recommended list of failure modes which should be considered in the safety analysis of vital electronic/software based equipment and systems used in safety-critical (vital) applications.

2. The program described in this Manual Part should be considered a guideline to Manufacturers and Railways involved in the development, manufacturing and utilization of vital electronic/software based equipment and systems used in safety-critical (vital) applications.

C. Reference Documents


7. CENELEC EN 50205 Relays with forcibly guided (mechanically linked) contacts.

D. Abbreviations

FMECA Failure Modes Effects and Criticality Analysis
PFU Probability of a Failure Being Unsafe
WCA Worst Case Analysis

CENELEC European Committee for Electrotechnical Standardization

E. Hardware Design Requirements

1. CLASS I Hardware (Vital Hardware)
   a. Vital hardware circuits shall be designed to enable exhaustive and comprehensive analysis using failure modes, effects, and criticality analysis (FMECA) techniques.

2. CLASS II Hardware (Non-vital Hardware Used To Implement Vital Functions)
   a. Hardware designated as CLASS II hardware shall be designed such that all credible failures, including secondary failures in combination with non-self-revealing initial failures, within that hardware shall be demonstrated, by analysis and/or tests, to either:

      (1) Have no unsafe effect on the implementation of vital functions; or
      (2) Be detected and, once detected, subsequent action shall assure that no unsafe effect is produced. In this case, the detection of failures that could have an unsafe effect shall be accomplished by continually proving that the failure has not occurred.
b. Functional Fault Trees (FFT) may be used to identify those failures that must be considered in CLASS II Hardware at a functional block level.

3. CLASS III Hardware (Hardware not used for Vital Functions)

   Hardware not used for the implementation of vital functions and not designated as either CLASS I, or CLASS II hardware shall be designated CLASS III.

   a. CLASS III hardware shall be designed so that it can be demonstrated that operation of or failure within that hardware has no effect on the safe implementation of vital functions.

4. Implementation of vital hardware shall specifically include separation of PCB traces and components, detailed specification of components, and the separation and demarcation between CLASS I, CLASS II and CLASS III circuits.

F. Analysis of CLASS I Hardware

1. An FMECA is required on all hardware designated as CLASS I (vital hardware). The minimum requirements of the FMECA are:

   a. All credible failure modes of all components shall be analyzed and/or tested by being induced or simulated on the physical hardware circuit, fabricated in final form. Simulation or engineering analysis may be used where physical testing is destructive or not achievable.

      (1) Component and circuit failure modes analyzed in the FMECA shall include as a minimum those specified in minimum requirements for the FMECA of CLASS I Vital Hardware below (Section I).

   b. The FMECA shall classify all failure modes as either self-revealing or non-self-revealing.

   c. The FMECA shall show that no single failure mode produces an unsafe condition.

   d. The FMECA shall show that all first level non-self-revealing failures in combination with subsequent failures produce no unsafe conditions. Engineering judgment shall be used to determine if additional level failures should be considered.
G. Analysis of CLASS II Hardware

1. An analysis shall be provided, at the functional block level, showing that all possible failures of CLASS II hardware which could adversely affect the safe implementation of vital functions have been accounted for by showing that either:
   a. the failure will have no unsafe effect on the implementation of vital functions, or
   b. the failure will be detected and once detected, subsequent action assures that no unsafe effect is produced.

2. The types of analyses provided depend upon the safety assurance concepts used, the system design, and the factors upon which safety assurance is dependent. The following requirements apply in providing analyses depending upon system design and factors on which safety assurance is dependent.

   a. Designs Incorporating Self-Checking

      In those systems in which safety assurance is dependent upon the identification of all failure modes and the effects of their occurrence being anticipated, the analysis shall show:

      (1) All credible failures that could adversely affect the safe implementation of a vital function have been anticipated. Functional Fault Trees as described in IEEE 1483-2000 may be used to identify the credible failures.

      (2) Any mechanism or test designed to detect the occurrence of each failure is effective in revealing the failure.

      (3) The reaction of the system, once the failure is revealed, maintains a safe state or states.

      (4) The mechanism or test used to reveal the failure and the subsequent system reaction to the occurrence of the failure cannot be compromised by the failure itself, or any subsequent failure or combination of failures, or by unrevealed errors in the software.

   b. Designs Incorporating Checked Redundant Comparison
In those systems in which safety assurance is dependent on hardware failures being revealed by comparison of independent hardware circuits, the analysis shall show:

(1) All credible failures that could adversely affect the safe implementation of vital functions are revealed by detecting differences in the points of comparison between the systems. Functional Fault Trees as described in IEEE 1483-2000 may be used to identify the credible failures.

(2) The comparison mechanism has no mode of failure that could compromise its ability to detect differences between the systems.

(3) The reaction of the system, once the failure is revealed, maintains a safe state or states.

(4) The mechanism or test used to reveal the failure and the subsequent system reaction to the occurrence of the failure cannot be compromised by the failure itself, or any subsequent failure or combination of failures, or by errors in the software.

c. Designs that Incorporate Numerical Assurance Techniques

The analysis of those systems in which safety is assured by the guarantee of an upper bound on the PFU shall show:

(1) The method used to calculate the PFU is valid and the calculations are accurate.

(2) All ancillary functions required to be performed for the PFU to be considered valid are performed correctly.

(3) All factors upon which the validity of the PFU depends are complete and correct.

(4) The mechanism and techniques used to verify numerical results are such that failures cannot reduce the value of the PFU of the processor-based system in which it resides.

(5) All failures that could adversely affect the safe implementation are included in the numerical coverage. Functional Fault
Trees as described in IEEE 1483-2000 may be used to identify the credible failures.

H. Analysis of CLASS III Hardware

An analysis shall be provided proving that operation of or failure within that hardware designated as CLASS III hardware within the system has no effect on the safe implementation of any vital function.

I. Minimum Requirements for the Failure Modes and Effects Criticality Analysis of Vital Hardware

1. As a minimum, the following failure modes and conditions shall be analyzed in the FMECA performed on all hardware designated as CLASS I hardware:

   a. Circuit operational modes not necessarily related to component failures, such as self-oscillation, acceptance of spurious signals, vulnerability to electrical or mechanical shock, and any phenomena that may mimic signals normally indicating safe conditions, shall be analyzed.

   b. Further, the effects of variations in power supply voltages, switching transients and ripple, and possible coupling of circuits through common power supply effects shall be analyzed, and the potential for abnormal circuit configurations that could occur as a result of the opening of circuits where three or more components are connected to a common node, shall be analyzed. (Opening of circuits implies that the trace connecting one of the components is opened without affecting the connection of the other components).

   c. Filters shall be analyzed to show that undesired signals are prevented from passing through the filter at levels that could cause unsafe conditions, even in the event of component failures within the filter.

   d. Sneak circuit paths, particularly those caused by components and/or wires connected to a common or by grounded nodes or common components or wires, must be considered.

   d-e. Multiple faults occurring from a common cause of these faults are considered a single failure. Potential common causes shall be considered to provide assurance that a multiple faults occurring as a result of a common cause, are safe.
combination of random single faults, and not as the result of a common cause fault.

2. Component Failure Modes

a. All failure modes listed could be intermittent. Intermittent failures are caused by environmental influences such as temperature variation or mechanical stress (see relevant environmental standards per Manual Part 11.5.1 Recommended Environmental Requirements for Electrical and Electronic Railroad Signal System Equipment). Therefore, the frequency of intermittent failures will be in accordance with these reasons (factors).

b. The following list of failures represents the MINIMUM analysis that should be performed, and any additional failures which are considered to be credible shall be added to the analysis. CENELEC 50129 may be used as a reference to consider additional failure modes, not necessarily complete, and any additional failure modes which are considered to be credible shall be added to the analysis.

c. Component failure modes shall be analyzed individually and shall include the following:

   Those failure modes marked with (*) below can be considered generally excluded from the analysis as non-credible only for the special components and under the specific conditions as described in Section I.2.e.(3).

   Those failure modes marked with (**) below can be justified in the analysis as excluded non-credible provided the items in I.2.e.(1) are satisfied. The considerations described in Section I.2.e.(4) may be used as part of that justification.

(1) Resistor
   (a) Open
   (b) Short(*)(**)
   (c) Resistance increase over plus tolerance(*), to open
(d) Resistance decrease under minus tolerance, to short(*)(**)

(2) Four Terminal Resistor

(e) Interruption of each terminal

(a)

(b) Interruption of resistance material(*)(**)

(c) Short circuit across the resistive element(*)(**)

(d) Increase of resistance value(*) of each terminal

(e) Decrease of resistance value(*)(**)

(f) Short circuit between two terminals of same side of the resistive element(*)

(f)

(3) Potentiometer

(a) Open

(b) Short

(c) Resistance increase over plus tolerance, to open

(d) Resistance decrease under minus tolerance, to short

(e) Increase in contact resistance of slider

(f) Change in division ratio

(4) Crystal or Crystal Oscillator

(a) Open Circuit

(b) Change in Frequency

(c) Short Circuit
(d) Short circuit to case, if the case is conductive.
(e) Decrease in Q

(4)(5) Diode
(a) Open
(b) Short
(c) Short to case, if the case is conductive
(d) Leakage current
(e) Consider effect of rectifying stray ac into circuit
(f) Decrease of reverse breakdown voltage
(g) Increase of forward voltage(**)
(h) Decrease of forward voltage(**)

(5)(6) Capacitor
(a) Open
(b) Short
(c) Increased leakage(**), to short
(d) Short to case, if the case is conductive
(e) Increased dissipation factor
(f) Increased capacitance(*)(**)
(g) Decreased capacitance(*)(**)

(7) Four Terminal Capacitor
(a) Interruption Open of each terminal
(b) Short circuit across the capacitive element
(c) Short to case, if the case is conductive

(d) Increase of capacitance(**)

(e) Decrease of capacitance(**)

(f) Increased leakage(**), to short circuit

(g) Increased dissipation factor

(h) Short circuit between two terminals of same side of the capacitive element(**)

(8) Light Emitting Diodes (LEDs)

(a) Open

(b) Short

(c) Decrease in light output at constant current

(d) Increase of leakage current

(e) Increase or decrease of forward voltage

(f) Change in LED color output

(g) Light emission below threshold voltage

(h) Light emission with reverse polarity

(i) Consider effect of rectifying stray ac into circuit

(6)(9) Zener Diode

(a) Open

(b) Short

(b) Short to case, if the case is conductive
(d) Reference voltage drift. Increase or decrease (both forward and reverse directions) voltage (**) 

(e) Reference voltage drift. Increase or decrease (forward and reverse directions) voltage (**) 

(f) Leakage current 

(g) Consider effect of rectifying stray ac into circuit 

(f) Increase of forward voltage 

(g) Decrease of forward voltage 

(7)(10) Transistor (other than Field Effect Transistors) 

(a) Open, each element to element. 

(b) Short, element to element and element to case, if case is conductive. 

(c) Leakage current, element to element and element to case, if case is conductive. 

(d) Increased gain (if not employed for switching) (**). 

(e) Decreased gain 

(f) Saturation voltage change 

(g) High frequency emitter-follower oscillation 

(h) Change of rise, fall, turn on, or turn off time 

(i) Increase of base-emitter threshold voltage 

(j) Decrease of base-emitter threshold voltage 

(11) Field Effect Transistor 

(a) Open, each element 

(b) Short, element to element and element to case
(c) Leakage current, element to element and element to case
(d) Increase of forward transconductance
(e) Decrease of forward transconductance
(f) Increase of gate threshold voltage
(g) Decrease of gate threshold voltage
(h) Change of turn-on-time and turn-off time
(i) Change of static drain to source on-state resistance

(8)(12) Thyristor
(a) Open, each element to element
(b) Short, element to element and element to case.
(c) Leakage current, element to element
(d) Change in holding current
(e) dv/dt false turn-on effects

(9)(13) Transformer
(a) Open primary
(b) Open secondary
(c) Turn-to-turn short, primary(*)
(d) Turn-to-turn short, secondary(*)
(e) Interwinding short(*)
(f) Winding to core short(*)
AREMA® C&S Manual

Part 17.3.3

(g) Signal feed-through with winding ground points opened (inter-winding capacitance feed-through)
(h) Increase of winding resistance
(i) Increase of inductance(**)
(j) Decrease of inductance(**)
(k) Change in transfer ratio(**)

(10) Inductor
(a) Open
(b) Short
(c) Turn-to-turn short(**)
(d) Winding to core short(**)
(e) Ratio of normal signal level to saturating signal level
(f) Increase winding resistance
(f)(g) Increase of inductance(**)
(g)(h) Decrease of inductance(**)

(11) Relays
(a) One or more Back back contacts fails to open when relay is energized
(b) One or more Front contacts fails to close when relay is energized
(c) One or more Back contacts fails to close when relay is de-energized
(d) One or more Front contacts fails to open when relay is de-energized(*)
(e) Change in timing characteristics
(f) Insulation failure, contact-to-contact or contact-to-coil, or contact to frame or ground.

(g) Arc suppression failure

(h) Excessive current on contacts

   Insulation failure, contact to frame or ground

   Insulation failure, coil to frame or ground

(g) Open, coil

(h) Increase contact resistance

(i) Increase pick-up current

(j) Decrease pick-up current

(k) Increase drop-away current

(l) Decrease drop-away current

Change of pick-up to drop-away ratio

Relay does not pick-up

Relay does not drop-away

(m) Closure of any front contact at the same time as any back contact (transient or continuous)(* )

Non-correspondence between front contacts

Non-correspondence between back contacts

(n) CChattering or fluttering of contacts

(o) Relay picks up if reverse polarity voltage is applied(**)

(12)(16) Fuse

(a) Open Circuit

(b) Failure to Open open when required(**)

(c) Increased Resistance
(13)(17) Jumper or Jumper Posts
(a) Short Circuit when required open
(b) Open Circuit when required short
(c) Low Resistance
(d) High Resistance

(14)(18) Optically Coupled Isolators
(a) No output
(b) Diminished band width (no response to higher frequency signals)
(c) Current transfer ratio degradation
(d) Intermittent operation
(e) Unstable detector stage amplification
(f) Increased detector stage leakage current
(g) Input to output short (**)
(h) Output stuck high
(i) Output stuck low
(j) Degradation of the isolation between input and output

(15)(19) Surge Arrestor
(a) Open Circuit
(b) Short Circuit
(c) Short circuit to conductive case
Part 17.3.3

200720176

(e)(d) Change in Breakdown\_breakdown Voltage\_voltage

(d)(e) Leakage Current\_current

(16)(20) Switch

(a) Open Circuit\_circuit or increased resistance, any contact

(b) Short Circuit\_circuit or Decreased\_decreased resistance, any contact

(c) Failure to Make\_Make

(d) Failure to Break

(17)(21) Multiple Components Connected to Common Bus

(a) Abnormal circuit configurations due to circuit openings at various points along the bus

(b) Abnormal return current paths and voltage drops due to openings at various points along the bus

(18)(22) Connector(s)

(a) Open Circuit\_circuit any pin

(b) Increased Resistance\_resistance

(c) Short between adjacent pins or to ground\(^*\) (pins separated by more than 0.25 in. surface leakage distance or those complying with the creepage and clearance requirements for reinforced insulation as specified in Reference 5 can be assumed not to short)

(d) Leakage between pins\(^*\)

(e) Leakage to ground\(^*\)

(f) Wrong mechanical position
(19)(23) Adjacent PC Board Traces

(a) Trace-to-trace shorts and shorts between connector contacts shall be considered component failure modes and shall be analyzed. Short or leakage between adjacent traces (including vias, through-holes, pads, etc.) (*)

(b) Short or leakage between adjacent layers at vias, through-holes and board edges (*)

(c) Abnormal circuit configurations that could occur as a result of the opening of circuits where three or more components are connected to a common node, excluding busses which are addressed in (201).

Opening of circuits implies that the trace connecting one of the components is opened without affecting the connection of the other components.

(a) Adjacent PCB traces and connector contacts conforming to the following minimum requirements may be exempted:

(i) For PCB components where wires connected to that circuitry leave the enclosure (or supply is not isolated):

1. Minimum spacing between traces or connector contacts not humisealed is 0.250 in or complies with the creepage and clearance requirements for reinforced insulation as specified in Reference 5.

2. Minimum spacing between humisealed traces is 0.100 in or complies with the creepage and clearance requirements for reinforced insulation as specified in Reference 5.
(ii) For PCB components connected to isolated power supplies (where no wires connected to that isolated circuitry leave the enclosure), the following trace spacings apply:

1. Minimum spacing between traces or connector contacts not humisealed is .050 in. or complies with the creepage and clearance requirements for reinforced insulation as specified in Reference 5.

2. Minimum spacing between humisealed traces is .025 in. or complies with the creepage and clearance requirements for reinforced insulation as specified in Reference 5.

(iii) For multi-layer boards

Layer to layer shorts do not need to be considered (except at vias and board edges, then the spacings listed above apply).

### b.d. Integrated Circuits

(1) Integrated Circuits (including microprocessors) cannot have all of their failure modes credibly predicted due to the device complexity. The following process shall be used for analysis of integrated circuits:

(a) All hazardous failure modes related to the functionality of the specific integrated circuit shall be determined using Fault Tree Analysis and Functional Fault Tree Analysis as described in IEEE 1483-2000.

(b) For each identified hazardous failure mode, an assessment and justification shall be made to show that either:

(i) The failure mode cannot credibly occur, due to the internal architecture of the integrated circuit, or
(ii) The failure mode will be externally detected and a safe state imposed.

(c) For integrated circuits and microprocessors, the following minimum list of failures shall be considered.

(i) Incorrect or ambiguous system inputs
(ii) Inputs not present at the prescribed time
(iii) Incorrect system outputs
(iv) Outputs not present at the prescribed time
(v) System output when necessary inputs are not present
(vi) Changed memory contents
(vii) Changed clock rate
(viii) Data not current
(ix) Failure to exit from loop
(x) Arithmetic error
(xi) Sign error
(xii) Entry to or exit from a routine at the wrong time
(xiii) Illegal entry to a routine
(xiv) Improper execution of instructions
(xv) Skipping of program segments
(xvi) Failure to reset upon command
(xvii) Failure to halt upon command
(xviii) Latent faults
(xix) Common cause faults

(xx) Transient faults

(xxi) Intermittent Faults

(xxii) Other faults particular to the specific technology.

(xxiii) High frequency oscillation on any pin.

(e-g.) Special Components

(1) Failure Modes of Special Components can be considered “not credible” and the relevant failure modes of those components may be excluded from the safety analysis. Satisfactory justification must be provided in order for these failure modes to not be considered credible. As a minimum, the justification must include the following:

(a) Theoretical explanation of any inherent physical properties or characteristics.

(b) Evidence of compliance that the component has been properly produced (e.g. compliance with recognized quality standards and any special manufacturing techniques/instructions required).

(c) Explanation of any special mounting arrangements or other precautions.

(d) Evidence that the failure mode will not occur as a result of component ratings (e.g. component must be de-rated, even under failure conditions, for use in the circuit).

(e) Results of tests to demonstrate fail-safe behavior of the component under adverse conditions such as adverse electrical and environmental conditions.

(f) Evidence of previous experience of reliance on the component for inherent fail-safety.
(2) Special components must be clearly identified as special safety components on schematics and assembly drawings.

(3) Generally Accepted Special Components

The following components have been generally accepted within the industry as having specific failure modes that can be considered “not credible”:

(a) Carbon film resistors and Metallized film resistor, MIL-PRF-55182 or MIL-PRF-39017 (e.g., RNC/RNR/RNN/RLR60, RNC/RNR/RNN/RLR65, and RNC/RNR/RNN/RLR70) may increase in resistance but will not decrease in resistance.

(b) Wire wound resistors, MIL Type RW-79, manufactured to Specification MIL-R-26E (e.g., RW/RWR-79), used in circuits in which their maximum dissipation does not exceed 10% of rated power, may decrease in resistance but will not increase in resistance except for a possible abrupt change to a value of 500 kilohms or higher. Note that the power dissipation limit must be maintained even in the event of failure of other components. If this is not the case, the described resistance characteristic does not apply.

(c) Wire wound resistors, MIL Type RWR-71, manufactured to Specification MIL-R-39007B, used in circuits in which their maximum dissipation does not exceed 10% of rated power (including fault conditions), will not vary in resistance more than ±5%. This acceptance characteristic requires in addition that (a) the resistors be mounted in a 4-terminal configuration which checks integrity of lead connection to external circuitry, (b) leads are formed under controlled conditions, and (c) the mechanical stability of resistor mounting is assured by suitable supports and tie downs.

(d) Capacitors, other than electrolytic type or units built up of separate capacitance elements connected in parallel and subject to loss of internal connections, will substantially retain the original capacitance value.
while the dielectric and structure are intact. However, film capacitors will exhibit an increase in capacitance if moisture penetrates the foil. This is always accompanied by an increase in dissipation factor and a decrease in insulation resistance. The increase in capacitance is about 10%. Then, if an increase in capacitance is a safety problem, a different type of capacitor, or a hermetically sealed unit should be used. The specification for the unit should call for 100% inspection of the enclosure.

Except for the above, two terminal capacitors may in all cases open, short and increase in leakage and dissipation. Four-terminal capacitors, properly installed, may be considered not to cause an unsafe or non-revealing failure when they fail open circuit.

4.(e) For Vital Relays built according to Manual Sections 6.1 and 6.2, Silver silver/carbon to silver contacts will not weld (stick). Therefore, a silver/carbon to silver front contact will always be open when the relay is in the de-energized position. In the event the silver to silver back contacts weld, the relay will not close its front contacts when energized.

(f) For Vital Relays built according to Manual Sections 6.1 and 6.2, biased neutral relays will not operate on reversed energy up to 50 times the value of relay working current, nor will they remain in the energized position if energy is reversed.

(g) Relays conforming to CENELEC EN 50205 may assume the failure mode of “Closure of any front contact at the same time as any back contact (transient or continuous)” is not-credible.

(h) Connector pins or adjacent PC board traces conforming to the following criteria may assume the failure mode of short to adjacent pins/traces is “not-credible”:

   (i) Minimum creepage spacing between pins or traces on outer layers of PC Boards is 0.250 in (6.35 mm)
Part 17.3.3

(ii) Minimum creepage spacing between conformal coated traces is 0.100 in (2.54 mm).

(iii) Minimum spacing between traces on the same interior layer of PC Boards is 0.100 in (2.54 mm).

(iv) For PCB components connected to isolated (floating) power supplies where no wires connected to that isolated circuitry leave the enclosure (i.e., are not exposed to the possibility of high voltage transients), minimum creepage spacing between pins or traces on outer layers of PC Boards is 0.050 in (1.27 mm).

(v) For PCB components connected to isolated (floating) power supplies where no wires connected to that isolated circuitry leave the enclosure (i.e., are not exposed to the possibility of high voltage transients), minimum creepage spacing between conformal coated traces is 0.025 in (0.64 mm).

For PCB components connected to isolated (floating) power supplies where no wires connected to that isolated circuitry leave the enclosure (i.e., are not exposed to the possibility of high voltage transients), minimum creepage spacing between traces on the same interior layer of PC Boards is 0.025 in (0.64 mm).

(vi)

(4) Other Component Failure Mode Considerations

The following considerations may be used in analyzing component failure modes provided the criteria in Section I.2.e.1 are met.
(a) Resistors conforming to the following criteria may assume the failure modes of short circuit and decrease in resistance are "not-credible" provided the criteria in Section I.2.e.(1) are also met will not occur:

(b) The body shall have no hollows.

(c) Creepage and clearance distances at each end of the component shall fulfill the requirements for conductor separation as identified in this document Manual Part.

(d) The coating shall be cement or enamel.

(e) The body shall be constructed of a non-conductive material, even at the highest temperature fault conditions within the ambient operating temperature range per Manual Part 11.5.1 Recommended Environmental Requirements for Electrical and Electronic Railroad Signal System Equipment.

(f) The coating shall be of a non-conductive material, even at the highest temperature fault conditions within the ambient operating temperature range per Manual Part 11.5.1.

(g) For wirewound resistors, the component shall have only 1 layer.

(h) For wirewound resistors, short circuited turns shall be possible to be eliminated by wire coatings and/or physical separation between turns.

(i) The resistance shall be limited to the lowest possible value.

(5) Four terminal resistors conforming to the following criteria may assume the failure mode of resistance material open circuit is "not-credible" provided the criteria in Section I.2.e.(1) are also met will not occur:

(a) Component must be constructed such that if a fault occurs causing interruption of the resistance material...
Part 17.3.3

occurs, that at least one of the four connecting terminals will also be interrupted open.

(b) The circuitry external to the four terminal resistor shall react in a failsafe manner in response to disclose the interruption of the open terminal(s) in a failsafe manner.

An example of the application of a four terminal resistor using a hybrid thick-layer technique is shown below in Figure 1733-1.

Figure 1733-1

(6) Four terminal resistors or four terminal capacitors conforming to the following criteria may assume the failure mode of a short circuit between two terminals on the same side is “not-credible” provided the criteria in Section I.2.e.(1) are also met will not occur:

(a) The two terminals on each side of the components shall be connected independently to each side of the component.

(7) Capacitors conforming to the following criteria may assume the failure mode of increased leakage is “not-credible” provided the criteria in Section I.2.e.(1) are also met will not occur:

(a) The component shall be designed for high voltage operation related to maximum operating voltage

(b) The component shall have Class Y1 specification per IEC 60384-14 and self-healing properties at the working source impedance and over the working voltage range. Ceramic Class Y1 capacitors are...
excluded because ceramic dielectrics are not self-healing and can have leakage and shorting failures modes.

(8) Capacitors (except electrolytic types) which can demonstrate that plate area, distance between plates, or dielectric constant cannot significantly change may assume the failure modes of increase or decrease in capacitance are “not-credible” provided the criteria in Section I.2.e.(1) are also met will not occur.

(9) Adjustable and non-adjustable inductors and transformers conforming to the following criteria may assume the failure modes of short circuits between windings, layers, turns, and body (including the core) are “not-credible” provided the criteria in Section I.2.e.(1) are also met will not occur:

(a) There shall be only 1 layer of turns separated by grooves in the body or by sufficient insulation (for example, insulation conforming to EN60950—Information Technology Equipment Safety).

(b) The turns, windings, and connections shall be securely fastened.

(c) Creepage and clearance distances between exposed conductors shall fulfill the requirements for conductor separation as identified in this Manual Part document.

(d) Power dissipation shall be limited sufficiently even under failure conditions, to prevent internal carbonization.

(10) Non-adjustable inductors and non-adjustable transformers conforming to the following criteria may assume the failure modes of an increase or decrease of inductance in any winding are “not-credible” provided the criteria in Section I.2.e.(1) are also met will not occur.
Part 17.3.3

(a) The magnetic core shall be constructed such that no significant change in reluctance of the magnetic path can occur (For example, core materials fracturing or cracking could decrease inductance).

(b) All criteria listed in Section 1.2.e.(9)(f) above.

(11) Non-adjustable transformers conforming to the following criteria may assume the failure mode of a change in transfer ratio is “not-credible” provided the criteria in Section 1.2.e.(1) are also met:

(a) All criteria listed in 6.I.2.e.(9)(f) and 7.(g)I.2.e.(10) above

(12) Optocouplers conforming to the following criteria may assume the failure mode of a short circuit in input to output is “not-credible” provided the criteria in Section 1.2.e.(1) are also met:

(a) Creepage and clearance distances shall fulfill the requirements for conductor separation as identified in this document.

(b) The construction of the component shall be robust and stable

(c) Power dissipation, even under fault conditions, shall be limited sufficiently to prevent internal carbonization

(d) Dielectric strength conforming to Manual Part 11.5.1 Recommended Environmental Requirements for Electrical and Electronic Railroad Signal System Equipment is satisfied.

(13) The gain of a transistor is dependent on doping levels, thickness of the junction(s), and lifetime of charge carriers. For a given temperature, the gain should only decrease with time.

(14) Fuses conforming to the following criteria may assume the failure mode of failure to open when required is “not-credible”
Provided the criteria in Section I.2.e.(1) are also met, will should not occur:

(a) The fuse and its holder shall be physically constructed and mounted so as to prevent the occurrence of a parallel short circuit.

(b) Means shall be provided to prevent the use of an incorrectly rated fuse.

(c) Means shall be provided to prevent the use of a fuse with self-resetting or self-healing capability.

The forward voltage of a diode or Zener diode is dependent on non-variable characteristics of the PN-p-n junction (charge carrier density, Boltzmann’s constant, electron charge) and should therefore be constant for a given temperature.

Connector pins or adjacent PC board traces conforming to the following criteria may assume the failure mode of short to adjacent pins/traces will not occur:

Minimum creepage spacing between pins or traces is at least 0.250 in.

Minimum creepage spacing between conformally coated traces is at least 0.100 in or complies with the creepage and clearance requirements for reinforced insulation as specified in CENELEC EN50129 (shall use overvoltage category IV).

For PCB components connected to isolated (floating) power supplies where no wires connected to that isolated circuitry leave the enclosure (i.e., are not exposed to high voltage transients), minimum creepage spacing between traces is at least 0.050 in.

For PCB components connected to isolated (floating) power supplies where no wires connected to that isolated circuitry leave the enclosure (i.e., are not exposed to high voltage transients), minimum...
creepage spacing between conformally coated traces is at least 0.025 in or complies with the creepage and clearance requirements for reinforced insulation as specified in CENELEC EN50129 (shall use overvoltage category OV2).
Recommended Procedure for Hazard Identification and Management of Vital Electronic/Software-Based Equipment Used in Safety-Critical (Vital) Applications

A. Purpose

This Manual Part provides a recommended procedure for hazard identification and management for vital electronic / software-based products and systems used in safety-critical (vital) systems. System/product developers may use it as part of the development process. End Users can use this as a guide to verify that proper development processes were followed.

The goals of a hazard analysis are:

1. Reasonably ensure that hazards associated with the functional requirements of the product or system are identified so that suitable mitigation methods or procedures are specified as a safety requirement of the product. Early stages of the development may use preliminary functional requirements.

2. Document what hazards were identified, and the results of an analysis of those hazards.

B. General

This Recommended Practice specifies three diverse procedures for identifying hazards at the system or application level. It does not however guarantee an inclusive list of all possible hazards. The effectiveness of the Hazard Analysis is directly related to how well and completely the functional requirements and the applications are defined, and how well this information is analyzed. Hazard Analysis in the early stages may use preliminary functional requirements.

Hazard Analysis refers to the process of identifying and analyzing hazards and hazardous events (see definitions in Manual Part 17.1.1 Definition of Terms Used in the Manual Parts in Section 17). Hazard logs are maintained to ensure that mitigation is developed and applied to reduce the hazard to a risk which is considered to be appropriate for the equipment and its intended use. This analysis usually will take place throughout the project, although the earlier it can be performed the less adverse impact it is likely to have.

Preliminary Hazard Analysis is primarily concerned with identifying hazards associated with the application of the product, and uses high level Fault Tree Analysis and other techniques. During preliminary hazard analysis a review of
potential hazards is systematically conducted. A Hazard Log is then created and initial entries are made in a Hazard List.

C. Abbreviations and Definitions

1. Definitions
   a. Safety authority: person who reviews and approves safety tasks.
   b. System/Product Developer (developer): the organization responsible for the development of the system/product design function and its associated safety documentation.
   c. System/Product Development Manager: person ultimately responsible for the system/product design.

2. Abbreviations
   PHA Preliminary Hazard Analysis
   PHL Preliminary Hazard List

D. Product Safety Classes

1. Classifications

   Traditionally, safety-critical railroad systems and the equipment that made up these systems have been classified as either “vital” or “non-vital”. It is useful however to define an intermediate level of safety integrity for systems and equipment that may contribute to a hazard while not leading directly to it. For the purposes of this safety hazard analysis, products and the projects that develop them must be classified into one of three safety integrity levels using the criteria in section D.2 below.

   The three classifications are: Safety-critical, Safety-related and Non-Safety-related.

   This Recommended Practice covers both Safety-critical and Safety-related product development projects; however Safety-related projects may have less rigorous standards applied to the mitigation of the hazard and to its verification.

   Safety assurance documentation must contain a justification of the product’s classification. Section D.2 below provides guidance on considerations for selection of the classification. Products may include functions of different classifications.
2. Safety Classification Determination

a. Products or systems that identify at least one hazard that could lead directly to a mishap are Safety Critical.

b. Products or systems which do not lead directly to a mishap but which may significantly increase the overall risk of a mishap are Safety Related.

c. Products or systems that have no safety implications are Non-Safety Related.

d. In determining the safety classification of the product, the following questions should be considered:

(1) Can a failure of this product lead directly to a mishap, or significantly increase the overall risk of a mishap? Is this product relied upon or in part to perform safety critical functions?

(2) Is the failure of another system required to coincide with the failure of this product in order to produce a hazardous event? What is the risk of such coincident failures?

(3) Is human error required to coincide with a failure of this product in order to produce a hazardous event? How likely is such an error to occur; does it involve a breach of a well established procedure?

(4) Could a failure of the product confuse or mislead a human operator (e.g. false indications, failure to provide a warning etc.), which could lead to a hazard?

(5) Can the product affect the security of prohibitions such as work permits, track blocks, etc.?

(6) Could warnings omitted from documentation, including application documents, lead to a hazard? Are users aware of the safety classification of the product?

(7) Is the product addressable, and could conflicting allocation of addresses lead to a hazard?
(8) Is the product safe in every application and situation in which it may be configured?

(9) Could the use of the product in applications for which it was not intended lead to a hazard?

(10) Could a non-safety related product be mistaken for safety-critical or safety-related equipment? Could it function the same as other safety-critical or safety-related equipment?

(11) Could data or commands collected, stored, transmitted or re-transmitted by the product lead to a hazard?

(12) Could the product endanger personnel installing, testing, operating, maintaining or working in close proximity to the product? (e.g. electric shock; physical shock; fire, explosive or toxic hazard during equipment failure; heavy weight; excessive noise; excessive heat or cold stress; etc.).

(13) Could the product adversely affect other safety-critical or safety-related systems or products that it will interface to, or be in close proximity to? (e.g. backfeed into critical circuits; defeat safety defenses such as critical message protection [e.g. defeat CRC protection, stale message protection, etc.]; produce excessive electromagnetic interference; affect power supplies, etc.).

E. Preliminary Hazard Identification

There are three procedures for identifying hazards at the system and application level that will make up the initial entries into the Hazard List. These are Fault Tree Analysis, Brainstorming and the Systematic Failure Prevention Checklist; and all three must be used unless otherwise agreed to. The Project Safety Engineer (PSE) is responsible for ensuring the identified hazards are incorporated into the Hazard list. Figure 1735-1 below shows the identification process.
1. Fault Tree Analysis (FTA)

A high-level Fault Tree Analysis of the system of which includes the product will be part will be conducted. This FTA will take as its starting point the top-most interface of the product with its environment, which will generally mean that consideration will be given to how the product relates to the railroad. For example, a signal system may have the initial hazards of...
collision and derailment; a crossing warning system may have the initial hazard of train-automobile collision. The high-level FTA should be conducted to at least the context level of the system (i.e. consideration should be given to all inputs, outputs, and stored states of the system).

The inputs to the FTA are the functional requirements of the system, expert knowledge of the system and its application, and the hazards of other projects (which may include reference to fault trees produced by other projects). It is essential that the functionality and application of the product be fully described for the FTA to be effective.

Each hazard identified by the FTA must either open a hazard sheet and be included in the hazard list, or be cross-referenced to an existing hazard sheet.

2. Systematic Failure Prevention Checklist

Systematic failures include errors in the specification, design, manufacture, installation, operation, maintenance and software faults of the product. It includes repair and product support. These are mostly attributed to “people errors” as a result of improper training or inadequate procedures or processes.

The implication of this is that there must be in place standards and procedures which if followed will reduce the probability of these systematic errors to an acceptable level. Again, ideally these standards and procedures should be validated against this requirement. In the absence of the data to validate them, the standards and procedures must pass the “reasonableness” test. That is, everything reasonable and prudent must be done to eliminate the possibility of an error that could lead directly to an unsafe condition. And, in the absence of standards or procedures the project safety plan must describe or identify procedures for this project that will be followed and which will reasonably ensure that there will be no errors that will could lead to an unsafe condition.

3. Brainstorming

One or more brainstorming sessions will be conducted. The objective of brainstorming is to identify hazards that are not identified by the FTA (which is a systematic approach to identifying hazards), and that are not part of the safety checklist (which has a historical basis).

The inputs to brainstorming are the functional requirements of the system, expert knowledge of the system and its application (including knowledge of
problems and reports of faults and failures with similar equipment or applications), and hazards from other projects. Brainstorming relies upon the knowledge of the participants, who must therefore be knowledgeable about the product or its application, and may include outside customers.

A hazard sheet will be created for each hazard identified by the brainstorming session as not being adequately covered by the existing hazard sheets. The Project Safety Engineer (PSE) is responsible for keeping records of the brainstorming sessions, including attendees’ names and what hazards were generated.

F. Hazard Log

1. Purpose and Scope of the Hazard Log
   a. The Hazard Log is a series of records for identifying, recording, tracking and verifying hazards and their mitigations for safety-critical and safety-related products, as well as identifying, recording, tracking and verifying safety-related matters. The main mechanism for recording and tracking is a series of records known as the Hazard Log. The initial entries in the hazard log are made when the Preliminary Hazard Analysis is conducted.
b. One of these records is the Hazard List, which is made up of general information on the product and a series of Hazard Sheets, one for each hazard identified. Figure 1735-2 illustrates the nested files of the Hazard Log.

2. Hazard Log Procedures
   a. The Product or system developer is responsible for compiling and maintaining the Project Hazard Log. This may be done either electronically or may be a paper-based log.
   b. Entries to the hazard log should be made as necessary.
   c. The Developer, or safety authority, is responsible for ensuring that adequate back-up arrangements are made such that the Hazard Log could be recreated (e.g. electronic copy, photocopy stored off-site etc).

3. Hazard Log Contents
   a. The Hazard Log either contains or references the following information:
      (1) Hazard Sheets

         Reference to the project hazard sheets will be contained in this section. A copy of the most recent Hazard Status Report will be included. The hazard sheet requirements will also be included. See Appendix B for a detailed description of the Hazard Sheet contents.

      (2) Hazard Change Log

         Reference to the Hazard Change Log along with a copy of the most recent activity will be included in this section. See Appendix C for a detailed description of the Hazard Change Log contents.

G. Hazard Risk Assessment

Each hazard identified in the hazard list is assessed for risk based on its severity category and probability category. It is recommended that hazard risk be assessed before any mitigation is applied. It is required that hazard risk be assessed after
mitigation has been applied (i.e. the residual risk).

1. Severity Category

Hazard severity categories are defined to provide a qualitative measure of the worst credible mishap resulting from personnel error; environmental conditions; design inadequacies; procedural deficiencies; or system, subsystem or component failure or malfunction. The following hazard severity classifications should be used when conducting safety analysis of systems:

**Table 1735-1**

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>CATEGORY</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CATASTROPHIC</td>
<td>1</td>
<td>Fatality, system loss, or severe environmental damage</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>2</td>
<td>Severe injury, severe occupational illness, major system or environmental damage</td>
</tr>
<tr>
<td>MARGINAL</td>
<td>3</td>
<td>Minor injury, minor occupational illness, or minor system or environmental damage</td>
</tr>
<tr>
<td>NEGLIGIBLE</td>
<td>4</td>
<td>Less than minor injury, occupational illness, or less than minor system or environmental damage</td>
</tr>
</tbody>
</table>

2. Probability Category

Hazard Probability is the probability that a hazard will be created during the planned life expectancy of the system that can be described in potential occurrences per unit of time. Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. A qualitative hazard probability may be derived from research, analysis, and evaluation of historical safety data from similar systems.

Supporting rationale for assigning a hazard probability should be documented in hazard analysis reports including any assumptions made. Recommended qualitative and quantitative hazard probability rankings are shown in the following table.
### Table 1735-2

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>LEVEL</th>
<th>Specific Individual Item (Qualitative)</th>
<th>Specific Individual Item (Quantitative)*</th>
</tr>
</thead>
<tbody>
<tr>
<td>FREQUENT</td>
<td>A</td>
<td>Likely to occur frequently</td>
<td>Greater than $10^{-3}$</td>
</tr>
<tr>
<td>PROBABLE</td>
<td>B</td>
<td>Will occur several times in the life of an item</td>
<td>Less than $10^{-3}$ and greater than $10^{5}$</td>
</tr>
<tr>
<td>OCCASIONAL</td>
<td>C</td>
<td>Likely to occur some time in the life of an item</td>
<td>Less than $10^{-5}$ and greater than $10^{7}$</td>
</tr>
<tr>
<td>REMOTE</td>
<td>D</td>
<td>Unlikely but possible to occur in the life of an item</td>
<td>Less than $10^{-7}$ and greater than $10^{9}$</td>
</tr>
<tr>
<td>IMPROBABLE</td>
<td>E</td>
<td>So unlikely, it can be assumed occurrence may not be experienced</td>
<td>Less than $10^{-9}$</td>
</tr>
</tbody>
</table>

* Probability of failure per operating hour.

The specific individual items, as referenced in the table, consist of a single controller (not a complete system) such as:

- Single Track Circuit (Transmitter and Receiver)
- Single Grade Crossing Motion Predictor
17.3.5

- Interlocking Controller (capable of controlling a double crossover)
- Single Carborne Controller (including capability for Movement Authority Display, Cab Signal, Over-speed protection, Positive Stop, Civil Speed enforcement).

The probability classification for an item that could be attributed to human error or the failure of a human to perform a particular procedure correctly should be considered as being frequent.

3. Risk Assessment

The risk associated with a hazard is a combination of the severity of the hazard and its probability of occurrence. The following table provides an example of the relationship between risk, severity and probability as it may be applied when assessing overall acceptability of products used in safety-critical (vital) applications. Individual suppliers and railroads may choose to modify this table to reflect existing procedures or requirements.

Table 1735-3

<table>
<thead>
<tr>
<th>HAZARD CATEGORY</th>
<th>(1) CATASTROPHIC</th>
<th>(2) CRITICAL</th>
<th>(3) MARGINAL</th>
<th>(4) NEGLIGIBLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>FREQUENCY</td>
<td>(A) FREQUENT</td>
<td>(B) PROBABLE</td>
<td>(C) OCCASIONAL</td>
<td>(D) REMOTE</td>
</tr>
<tr>
<td>(A) FREQUENT</td>
<td>1A</td>
<td>2A</td>
<td>3A</td>
<td>4A</td>
</tr>
<tr>
<td>(B) PROBABLE</td>
<td>1B</td>
<td>2B</td>
<td>3B</td>
<td>4B</td>
</tr>
<tr>
<td>(C) OCCASIONAL</td>
<td>1C</td>
<td>2C</td>
<td>3C</td>
<td>4C</td>
</tr>
<tr>
<td>(D) REMOTE</td>
<td>1D</td>
<td>2D</td>
<td>3D</td>
<td>4D</td>
</tr>
<tr>
<td>(E) IMPROBABLE</td>
<td>1E</td>
<td>2E</td>
<td>3E</td>
<td>4E</td>
</tr>
</tbody>
</table>

Hazard Risk Index

1A, 1B, 1C, 2A, 2B, 3A  Suggested Criteria
1D, 2C, 3B, 4A  Unacceptable
1E, 2D, 3C, 3D, 4B, 4C  Undesirable

Acceptable with review
Risk classifications should be applied as follows:

- **Unacceptable.** Products with residual risks rated at this level are not considered acceptable.

- **Undesirable.** Products with residual risks rated at this level are not desirable. Depending on economic and functional requirements, equipment or systems with hazards rated at this risk level may be considered acceptable with explicit agreement from the product user.

- **Acceptable With Review.** Depending on economic and functional requirements, equipment or systems with residual risks rated at this level may be considered acceptable with notification to the user.

- **Acceptable without review.** Additional design effort or product revision is not required to reduce the severity or probability of hazards with this risk level.

### H. Hazard assignment and completion

1. Assigning hazards

The safety authority identifies which functional group (e.g. design, manufacturing, application, etc.) is responsible for developing the mitigation for a particular hazard, and then assigning the hazard to a responsible individual in that area. This assignment shall be recorded, and must be confirmed with the people assigned the hazards.

2. Assignee accepts hazard

It is important that the assignee understands the hazard, and is in a position to be able to answer the hazard. The assignee should consider the context of the hazard very carefully as well as any initial risk assessment. Care should be taken to not increase the scope of the hazard too widely, or to make an overly restrictive interpretation of the hazard.

3. Hazard completion

When the defense mitigation has been developed it must be clearly stated on the hazard sheet in sufficient detail to be able to verify that it does in fact exist, and that it does reduce the risk to an acceptable
level. In cases where no mitigation is required the justification for reaching that decision must be stated on the hazard sheet.

The assignee is required to perform a risk assessment based on the hazard with the mitigation applied (mitigated risk assessment), using the techniques described in this document. The assignees should take care to record any assumptions or particular interpretation that they have made concerning the hazard or the mitigation.

Some potential sources of mitigation include:

- Hardware or software defenses, protection devices or inherently fail-safe components
- Design or verification and validation techniques (e.g. testing, reviews, etc.)
- Cautions, Warnings and instructions in user and application manuals
- Standards, procedures, policies
- Manufacturing checks and tests
- People related defenses (e.g. experienced staff, trained staff, etc.)

4. Hazard management

The safety authority is responsible for maintaining the hazard list during the project, adding new hazards as they arise, reassigning hazards as necessary, collecting, controlling and submitting hazards to the approval process.

5. Approval

The approval process requires agreement from the System/Product Development Manager and the safety authority. Both must agree that the mitigation is adequate (i.e. the defense as implemented reduces the risk to the desired level) and has been implemented correctly before the hazard sheet can be approved and the status of the hazard can be changed to "Closed". The safety authority is responsible for verifying that the mitigation has been implemented in the final product.

6. Unresolved Hazards
A product with an unresolved hazard, or a residual risk assessed as undesirable, must not be placed in service unless the customer is formally made aware of the risks in writing.
Appendix A: Hazard Mitigation Process

Step 1
Hazard Distribution

Step 2
Determine whether you understand the hazard.
Yes
No

Step 2a
Consult with safety authority

Step 3
Determine whether it is reasonable that the hazard is assigned to yourself
Yes
No

Step 3a
Consult with safety authority

Step 4
Complete the Hazard Mitigation
Mitigation
Reference Documents
Mitigated Risk Assessment

Step 5
Indicate Hazard is ready for collection by changing status to "Pending".

Step 6
Collection of Hazard

Step 7
Collected Hazard placed under configuration control.

Step 8
Hazard Checked

Step 9
Hazard Acceptable
Yes
No

Step 9a
Hazard Corrected

Step 10
Hazard Closed
Figure 1735-3: Hazard Mitigation Process
Appendix B: Hazard Sheet Content

The minimum required content of the hazard sheet is shown below:

- Hazard Sheet Reference. A unique reference identifier used to identify the hazard.
- Date that the hazard sheet was opened and entered in the log.
- Name of person that this hazard has been assigned to.
- Name of other people that this hazard has also been assigned to.
- Project being addressed by this analysis. Include system or sub-system name if appropriate.
- A description of the hazard.
- Probability and Risk categories. Risk justification should be provided if necessary.
- Mitigated Severity, Probability and Risk categories. Risk justification should be provided if necessary.
- Mitigation. The safety features, defenses, procedures, or circumstances that prevent the hazard from occurring or that reduce the risk to an acceptable level. Where the risk is judged to be acceptable without additional action this section should state so and justify.
- Status. One of:
  - Assigned:
    Responsibility has been assigned but the mitigation method is not yet in a state that is suitable for review.
  - Pending:
    Mitigation method proposed, and the assignee has indicated to the PSE that the hazard mitigation is ready for review.
  - Pending under configuration control:
Mitigation method proposed, and is placed in a controlled state in preparation for review, but is not yet approved. The hazard may also be in this state if it is being updated as a result of a review.

- **Closed:**
  
  Potential hazard resolved, either by the mitigation, or the risk associated with the hazard was judged to be acceptable. The approved hazard is in a controlled state.

- Documents or references that support the mitigation should be listed. This section is used as a means to verify the mitigation, and should refer to specification and design documentation, as well as appropriate standards and procedures.

- Any relevant comments. This may include further clarification or interpretation of the hazard being mitigated, names of people who were consulted in connection with the hazard, or suggestions for future improvement for example.

- Approval and dates. The System/ Product Development Manager and the safety authority will indicate their approval of the mitigation by checking the corresponding box next to their name. The hazard will not be closed until both boxes have been checked indicating approval by each.

**Appendix C: Hazard Change Log Content**

The automatically created hazard change log text file from the hazard mitigation database can be used or a manual hazard change log containing the following information for each change will be sufficient to satisfy this requirement:

- Date of change,
- Hazard ID,
- Hazard Assignee,
- New change description,
- Old description information before change.
A. Purpose

This Manual Part recommends a configuration management program for the in-service executive and application software configuration items used in vital signal applications.

While some executive and application software may be classified and considered as non-vital, its use as part of a control system used in vital signal applications may, consistent with the policies of the railroad, make it subject to the recommendations of this Manual Part.

B. References

1. See AREMA® Manual Part 17.1.1 Definitions of Terms Used in the Manual Parts Contained in Section 17 for definitions applicable to configuration management.

2. Also see AREMA® Manual Part 17.5.1 Recommended Configuration Management Program for Electronic and/or Software-Based Products Used in Vital Signal Applications for a description of the configuration management program to be used by suppliers and railroads during the development and release phases of electronic/software-based products in general.

C. Recommended Configuration Management Plan for Railroads

These recommendations represent one method of providing configuration management and control of software items utilized by railroads. The actual configuration management plan used may vary depending upon the individual railroad, its size, organizational structure and the inventory of electronic and/or software-based signal products.

1. Executive Software

   a. The master source (e.g. PROM, data file, etc.) of the executive software should be obtained only from the supplier (the Original Equipment Manufacturer, or OEM) of the product, or alternate approved source. The executive
software should not be modified or changed by anyone other than the OEM.

a. Railroad personnel should make copies of the executive software for various locations only from the master source, subject to the policies of the OEM and the railroad.

b. Only versions of executive software approved by the appropriate authority within a railroad should be provided to field maintenance personnel.

c. Employees shall ensure that the executive software of a given version loaded into various locations is the correct version (e.g. has the same Checksum or Cyclic Redundancy Check (CRC)) as the master source, or is installed using a Unique Check Number (UCN).

d. When installing a new version of executive software, the appropriate labels should be verified, where applicable.

2. Application Software

a. Application software may be developed by the railroad, supplied by the OEM, or other third party, and should be subject to a documented revision control procedure.

b. Employees shall ensure that the application software version loaded into a given location is the correct version (e.g. has the same Checksum or Cyclic Redundancy Check (CRC)) as the master source, or is installed using a Unique Check Number (UCN).

c. Application software shall not be loaded remotely into an in-service location.

d. Modifications to the application software shall not be implemented at field locations for any purpose without verification and testing. Implementation of patches or other program changes shall be verified and approved by the appropriate authority within a railroad responsible for quality assurance before they are placed in service.
e. When installing a new or revised version of application software, the appropriate labels shall be updated, where applicable.

3. Additional Considerations - Requirements for Railroads

   a. When a railroad orders a new or revised software function from the OEM or third party, a written description of the required functionality (or operational changes in the case of revised software) should be developed. The written description should also be sent to the attention of the appropriate authority within the railroad responsible for quality assurance for the applicable territory. This description shall be used to verify the new software when it is received. All new or revised software should be accompanied by the following documentation:

   (1) Functional Description
   (2) Change Summary
   (3) Electro-mechanical or electronic software/chassis keying information, as applicable.

   b. The authority responsible for configuration management shall provide a secure storage location for master source and supporting documentation for both executive and application software. The master source of all application and executive software (regardless of the storage media) should be stored from receipt and for a period of time not less than 12 months after all copies of the software version have been removed from service.

   c. A master list of all approved software and copies of associated documentation should be kept and updated as new versions are approved. The list should be distributed and made easily available to all field forces.

   d. Every field location receiving new or revised software shall be subjected to an operational test before being declared in-service. Any operational tests performed should be
documented and a copy of the test sheets and test results filed for future reference.

A record should be kept for all installations where software-based equipment is used. This should be used to record all software revision information installed at the location. As applicable, the record for a new or revised software version should include:

e.  

   e.  

   (1) Product Name
   (2) Equipment Type
   (3) Subdivision and Milepost
   (4) Software Revision Level or Version Number
   (5) Software Revision Date
   (6) Program Name
   (7) PROM Checksum, CRC, or other unique identifier
   (8) Manufacturer's Part Number
   (9) Date(s) Software Tested/Placed in Service
   (10) Employee(s) Sign Off (Initials)
   (11) A description of what changed

f. All obsolete or superseded software versions (including hardware implementations (e.g. PROMS)) should be removed from field locations and be clearly marked as obsolete. An example would be by drawing an indelible “X” across the label and immediately returning software to the appropriate authority within the railroad. Obsolete or superseded software shall not be re-installed in field equipment, unless authorized by the appropriate authority within the railroad.

g. Equipment designed to provide a visual display of software configuration information shall have such information verified
each time the equipment is turned on or as appropriate if the configuration display information can be manually requested.

h. For equipment that provides both application and executive software in a single data file (or PROM) the software shall be treated as executive software.

i. When replacing printed circuit boards that contain executive or application software, ensure that the proper revision or version level of the software is contained in the boards.

j. When ordering printed circuit boards and software, specify the required version.

k. Software should be duplicated using only supplier-recommended procedures and materials.

4. Additional Considerations - Requirements for Suppliers

a. Suppliers should provide the railroad with recommended procedures to be followed when duplicating executive or application software. Suppliers should provide the railroad with an approved list of storage media that may be used by the railroad when storing, transporting and duplicating application and executive software.

b. Supplier should provide compatible versions of boot software or other software development tools to allow uploading the executive and application software into hardware.

c. Supplier should provide notification of compatible versions of hardware and software.

d. Source code and all relevant documentation for all software releases provided by the supplier shall be maintained by the supplier in a secure location with appropriate version control protection. Each release should be maintained for a period of time not less than 12 months after the railroad provides notification that all copies of the release are removed from service.

e. Suppliers should provide written notification to and receive written acknowledgement from the proper authority at the
railroad prior to destroying archived software source code and relevant documentation.

f. The supplier, upon verification of the potential risks and development of either an interim or final solution, shall promptly notify the railroad of any safety-critical issue or condition due to a defect with equipment or software that may affect safe railroad operations. Notification shall indicate all affected hardware and/or software revisions, including a recommended course of action to be followed by the railroad.

g. Labeling by the Supplier

All application programs should contain the following information either on label or within the data file:

1. Product name (may be abbreviated)
2. Equipment type (where more than one type of the equipment exists)
3. Executive or Application software name
4. Software revision or version number
5. Checksum, CRC or other unique identifier
6. Date of software revision or version
7. PROM location on printed circuit board (IC number), if used.