Recommended Procedure for Hazard Identification and Management of Vital Electronic/Software-Based Products Used in Safety-Critical (Vital) Applications

Revised 2025 (15 Pages)

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) applications. 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 system/product lifecycle, 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 must be assigned to one of three safety classifications 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 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 have 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.

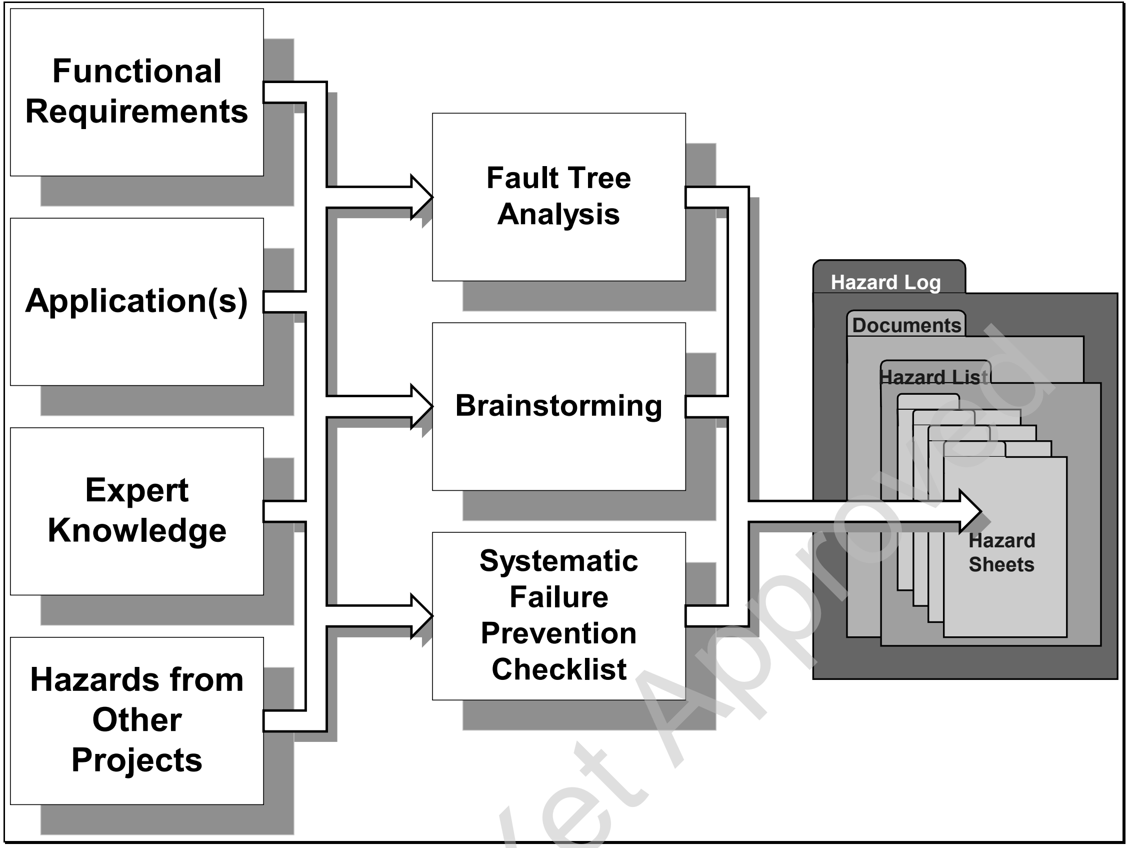

Figure 1735-1: Preliminary Hazard Identification

1. Fault Tree Analysis (FTA)

A high-level Fault Tree Analysis of the system which includes the product 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 products (which may include reference to fault trees produced for other products). 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 is that there must be in place standards and procedures which will reduce the probability of these systematic errors to an acceptable level. 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. In the absence of standards or procedures the project safety plan must describe or identify procedures that will be followed to reasonably ensure that there will be no errors that 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, 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 PSE is responsible for keeping records of the brainstorming sessions, including attendees’ names and what hazards were generated.

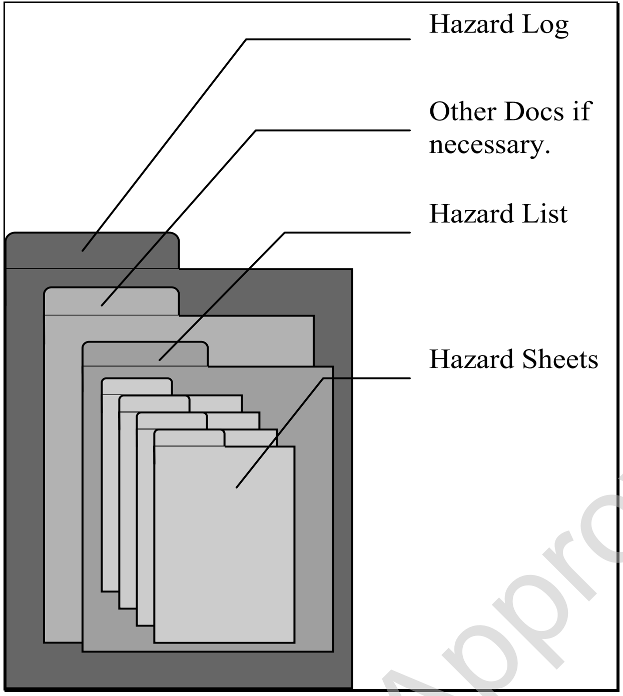

Figure 1735-2: Hazard Log

F. Hazard Log

1. Purpose and Scope

   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. 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 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

See Appendix B for a detailed description of the Hazard Sheet contents.

(2) Hazard Change Log

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

DESCRIPTION	CATEGORY	DEFINITION
CATASTROPHIC	1	Fatality, system loss, or severe environmental damage
CRITICAL	2	Severe injury, severe occupational illness, major system or environmental damage
MARGINAL	3	Minor injury, minor occupational illness, or minor system or environmental damage
NEGLIGIBLE	4	Less than minor injury, occupational illness, or less than minor system or environmental damage

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

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

* Probability of failure per operating hour.

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

a. Single Track Circuit (Transmitter and Receiver)

b. Single Grade Crossing Motion Predictor

c. Interlocking Controller

d. Single Carborne Controller (including capability for Movement Authority Display, Cab Signal, Overspeed 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

HAZARD CATEGORY FREQUENCY	(1) CATASTROPHIC	(2) CRITICAL	(3) MARGINAL	(4) NEGLIGIBLE
(A) FREQUENT	**1A**	**2A**	**3A**	**4A**
(B) PROBABLE	**1B**	**2B**	**3B**	**4B**
(C) OCCASIONAL	**1C**	**2C**	**3C**	**4C**
(D) REMOTE	**1D**	**2D**	**3D**	**4D**
(E) IMPROBABLE	**1E**	**2E**	**3E**	**4E**

Hazard Risk Index	Suggested Criteria
1A, 1B, 1C, 2A, 2B, 3A	Unacceptable
1D, 2C, 3B, 4A	Undesirable
1E, 2D, 3C, 3D, 4B, 4C	Acceptable with review
2E, 3E, 4D, 4E	Acceptable without review

Risk classifications should be applied as follows:

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

b. 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.

c. 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.

d. 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 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:

a. Hardware or software defenses, protection devices or inherently fail-safe components

b. Design or verification and validation techniques (e.g., testing, reviews, etc.)

c. Cautions, Warnings and instructions in user and application manuals

d. Standards, procedures, policies

e. Manufacturing checks and tests

f. People related defenses (e.g., experienced staff, trained staff, etc.)

4. Hazard management

The Safety Authority is responsible for maintaining the hazard list throughout the product lifecycle, 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

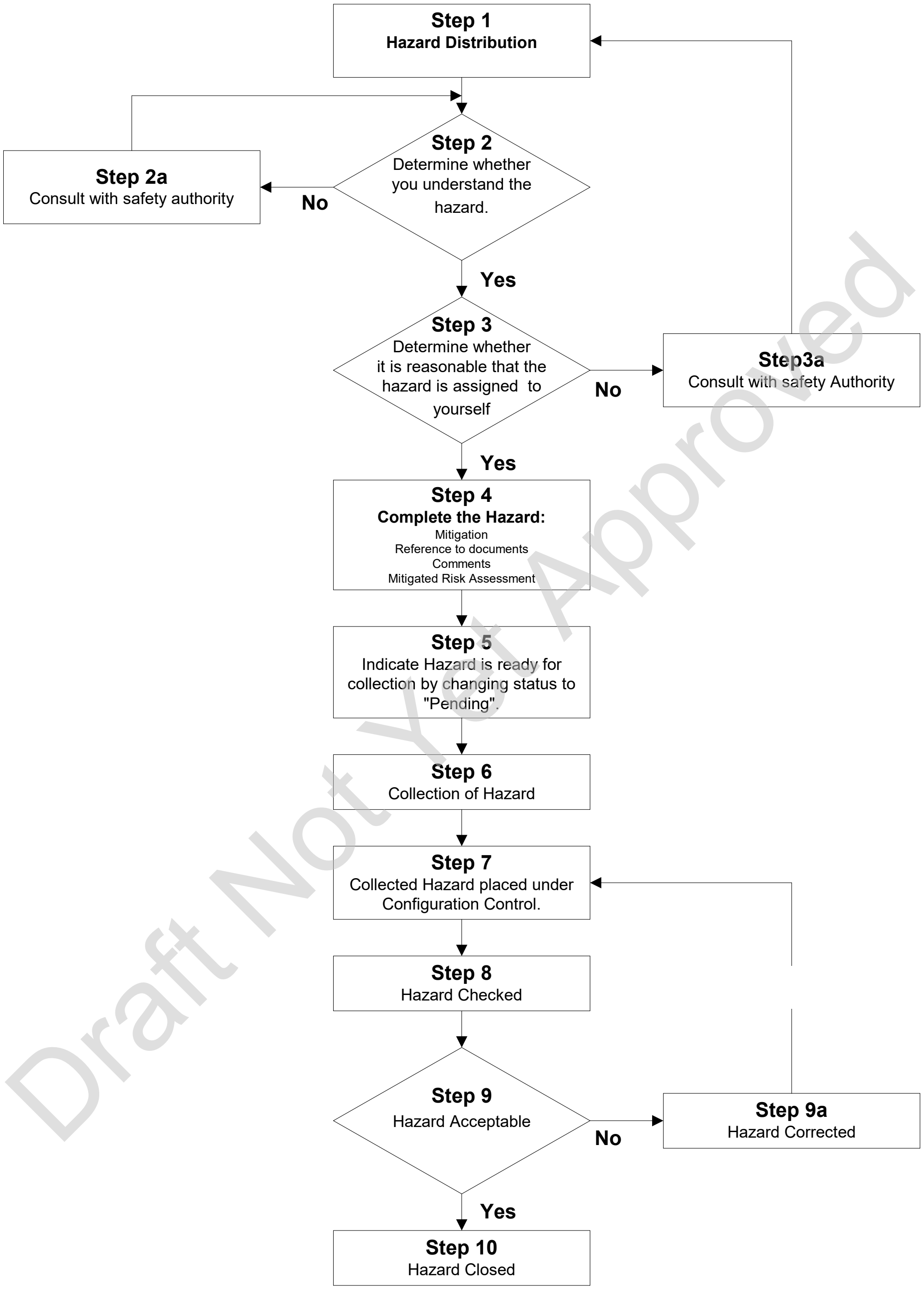
Step 1
Hazard Distribution
Step 2
Determine whether you understand the hazard.
No
Step 2a
Consult with safety authority
Yes
Step 3
Determine whether it is reasonable that the hazard is assigned to yourself
No
Step3a
Consult with safety Authority
Yes
Step 4
Complete the Hazard:
Mitigation
Reference to documents
Comments
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
No
Step 9a
Hazard Corrected
Yes
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:

1. Hazard Sheet Reference. A unique reference identifier used to identify the hazard.

2. Date that the hazard sheet was opened and entered in the log.

3. Name of person that this hazard has been assigned to.

4. Name of other people that this hazard has also been assigned to.

5. Project being addressed by this analysis. Include system or sub-system name if appropriate.

6. A description of the hazard.

7. Probability and Risk categories. Risk justification should be provided if necessary.

8. Mitigated Severity, Probability and Risk categories. Risk justification should be provided if necessary.

9. 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.

10. Status. One of:

    a. Assigned:

       Responsibility has been assigned but the mitigation method is not yet in a state that is suitable for review.

    b. Pending:

       Mitigation method proposed, and the assignee has indicated to the PSE that the hazard mitigation is ready for review.

    c. 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.

    d. 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.

11. 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.

12. 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.

13. 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:

1. Date of change,

2. Hazard ID,

3. Hazard Assignee,

4. New change description,

5. Old description information before change.