Table of Contents

11. Hazard Log

ASEMS Document Version:
4.3
Effective From:
Tuesday, 7 June, 2022 - 00:15
Summary:
This procedure provides guidance for the continual recording of hazards, accidents and accident sequences, including risk management information, in the Hazard Log.

11.1. Introduction

11.1.1. Definitions

11.1.1.1.

A **Hazard Log** is defined in Def Stan 00-056 [1] as:

“The continually updated record of the Hazards, accident sequences and accidents associated with a system. It includes information documenting risk management for each Hazard and Accident.”

11.1.2. Objectives

11.1.2.1.

The Hazard Log contains the traceable record of the Hazard Management process for the Project and therefore:

1. Ensures that the Project Safety Programme uses a consistent set of Safety information;
2. Facilitates oversight by the Project Safety Committee (PSC) and other stakeholders of the current status of the Safety activities;
3. Supports the effective management of possible Hazards and Accidents so that the associated Risks are brought to and maintained at a tolerable level;
4. Provides traceability of Safety decisions made.

11.1.2.2.

These Hazards, accident sequences and accidents are those which could conceivably happen, and not only the ones which have already been experienced.

11.1.2.3.

The term Hazard Log is considered by some as somewhat misleading, because the information stored relates to the entire Safety Programme and covers accidents, controls, Risk Evaluation and ALARP justification, as well as data on hazards.

11.1.2.4.

Outstanding issues in the Hazard Log will be regularly reviewed by the Project Safety Committee to make sure that actions are completed and unacceptable risks are resolved.

11.2. Procedure

11.2.1. Hazard Log Fundamentals

11.2.1.1.

The Key features associated with the Hazard Log are identified below:

1. The Hazard Log is a live document and as such will be updated throughout the programme. The Hazard Log should be set up at the initial stages of a project and remains current throughout the CADMID/T life cycle of a Product, System or Service;
2. The Hazard Log will provide a record of all safety assessment information and evidence associated with

a programme;
3. The Hazard Log will provide documentation of all Safety Risk Evaluations conducted on a programme;
4. The Hazard Log will provide an auditable tracking mechanism for a programme, showing what decisions were taken, when and why;
5. The Hazard Log will provide a cross reference to all other Safety Analysis and documentation for a programme.

11.2.2. Content of Hazard Logs

11.2.2.1.

Typical Hazard Log contents are described in Further Guidance - Hazard Log Contents.

11.2.2.2.

The Hazard Log should describe the system to which it relates, and record its scope of use, together with the safety requirements.

11.2.2.3.

When Hazards are identified, the Hazard Log will show how these hazards were evaluated and the resulting residual risk assessed, and will either recommend further action to mitigate the hazards, or formally document the acceptance of these hazards and the ALARP justification.

11.2.2.4.

The Hazard Log is a structured way of storing and referencing safety Risk Evaluations and other information relating to an equipment or system, it will be co-ordinated and controlled whilst maintaining an auditable record of that information. It is the principal means of tracking the status of all identified hazards, decisions made and actions undertaken to reduce the risk and should be used to facilitate oversight by the Project Safety Committee and other stakeholders.

11.2.2.5.

The Hazard Log is a tracking system for hazards, their closures, and residual risk and should be maintained throughout the system life cycle as a “live” document. As changes are integrated into the system, the Hazard Log should be updated to incorporate added or changed hazards and the associated residual risk to reflect the current design standard.

11.2.2.6.

The Hazard Log should capture the inputs to and outputs from Hazard Analysis and Risk Evaluation sessions. ALARP justification arguments and conclusions should be recorded when mitigation actions are complete.

11.2.3. Designing the Hazard Log

11.2.3.1.

The process for a Hazard Log requires a number of initial steps to be undertaken prior to Hazard Log population. This is to ensure that there should be a suitable infrastructure in place before Hazard information is stored.

1. A method by which the Hazard Log is to be implemented should be selected; this can either be in paper or electronic form. It is important at the outset to identify the appropriate tool/administration method for the Hazard Log;
2. A Hazard Log administrator should be appointed. The Hazard Log administrator will be responsible for the maintenance, upkeep and configuration control of the Hazard Log. All non-administrators should be allowed read only access if the Hazard Log is in electronic format;
3. The Hazard Log should be ‘set up’. This will include activities such as inclusion of the Risk Classification scheme that has been agreed, determination of appropriate Hazard categories, status definitions and general set up activities to ensure that the Hazard Log will operate as required. The latter may be in the form of a guidance note for a paper based system or checking of the robustness of an electronic system.

11.2.4. Starting the Hazard Log

11.2.4.1.

Once the system and its boundaries have been defined and the Hazard Identification process has begun, the Hazard Log should be established in order to keep a record of the hazards and proposed or implemented

mitigation measures to ensure that the hazards are being appropriately controlled.

11.2.5. Running and Using the Hazard Log

11.2.5.1.

The Hazard Log should be the configuration control mechanism for the Safety Assessment process, and hazards should not be deleted from the Hazard Log, but closed and marked if no longer relevant. A procedure should be defined for the management and control of the Hazard Log. The Hazard Log should be retained for the entire system life cycle and it should act as the primary source of the Logical arguments, or Safety Case, for the deployment of the system into service.

11.2.5.2.

The Hazard Log should be reviewed at regular intervals to ensure that hazards are being successfully managed and that the robustness of the established safety arguments in the Safety Case are not being compromised.

11.2.5.3.

Generally the Hazard Log should be updated whenever:

1. A relevant Hazard or potential accident is identified, either through formal analysis or as a result of a change to the design, procedure or operating environment;
2. A relevant incident occurs, perhaps during testing or demonstration;
3. Further information relating to existing Hazards, incidents or accidents comes to attention; or safety documentation is created or re-issued.

11.2.5.4.

In order to provide project awareness of hazard and accident data, the Hazard Log should be accessible to all of the appropriate project staff. This should include, but not necessarily be limited to the Project Safety Panel.

11.2.5.5.

The Hazard Log shall be available for inspection by the Safety Auditor, the Safety Assessor and representatives of any relevant Safety Authorities or Defence Regulators.

11.2.6. Hazard Log Process

11.2.6.1.

Since the Hazard Log is a repository for managing identified hazards, it is possible for Hazard identification to begin prior to the implementation of the Hazard Log.

11.2.6.2.

Once the initial steps have been undertaken, the process of information entry should be started. The generic flow of the process is shown in the following steps:

1. Hazard Identification – Initially taken from procedures such as Preliminary Hazard Analysis, and should then be augmented by subsequent Risk Management activities;
2. Accident sequence should be developed in associated with the identified hazards;
3. A formal Risk Evaluation of each accident sequence should occur;
4. Mitigation identification – The appropriate and agreed mitigation for each accident should be recorded;
5. Mitigation/control owners established – This should ensure that the mitigation or controls identified are put in place and the hazard is addressed;
6. Cross checking should take place to see if there are any other, previously identified Hazards or accident sequences linked with this hazard;
7. Resolution – Status changes should be completed as required, formal closures recorded, including reference to evidence and ALARP justification recorded;
8. Ongoing hazards should be managed and new hazards added as required;
9. A Hazard Log Report as determined by the Project Safety Plan should be produced.

11.2.6.3.

Where the Project Safety Programme identifies hazards that are the responsibility of another Project, then the information should be passed to the person with delegated authority for that area. The Project Hazard Log will record that this was done.

11.2.6.4.

Because hazards and accidents usually have a range of control measures of different types associated with them, there is no single hazard “owner” who is responsible for mitigating the associated risks, other than the overall delegated authority. When a control measure is agreed for implementation, it should be clearly assigned to an “owner”. This might be the Prime Contractor for a design change, the Training Authority for a topic to be covered in Maintainer training, or the User for a procedural control solution.

11.2.7. Closure or Removal of Entries

11.2.7.1.

It should be best practice for the Hazard Log to record each Hazard as “open” and for ALARP arguments to be provisional until all mitigation actions are confirmed to be satisfactorily completed. An example is where the mitigation depends upon production of an operational procedure that may not be written for a considerable time after the Hazard is first identified at an early stage of design or construction. However, equipment should not be declared operational (or used in any scenario where it may present a hazard, e.g. trials) with risks that have not been formally declared ALARP. In the Military context, this may exceptionally mean declaring ALARP with mitigation measures outstanding. In such circumstances, and only when strict guidelines have been followed, ALARP may be declared.

11.2.7.2.

Hazards should not be deleted from the Hazard Log, but closed and marked as “out of scope” or “not considered credible”, together with the justification. Where they are no longer considered relevant to the system, the Log entry should be updated to reflect this.

11.2.8. Archiving on Project Closure

11.2.8.1.

At the end of the project, the Hazard Log should remain as a historical record, which should be useful to refer to for similar applications in the future.

11.2.9. Records and Project Documentation

11.2.9.1.

Adequate provision should be made for security and backup of the Hazard Log and other safety records.

11.2.9.2.

The Hazard Log is a prime source of corporate knowledge and is the configuration control mechanism for the Safety Assessment process. As such it could be referred to in legal proceedings. Every effort should therefore be made by the Project to ensure that records are accurate, attributable, up to date and complete. Clear cross-referencing to supporting documents is essential.

11.2.9.3.

Where relevant, the outputs from this procedure should feed into the following:

1. System Requirements Document – for any specific Safety requirements;
2. Customer Supplier Agreement – to document agreements on Safety information to be delivered by the Delivery Team;
3. Through Life Management Plan;
4. Safety elements of Outline Business Case and Full Business Case submissions.

11.2.10. Warnings and Potential Project Risks

11.2.10.1.

The relationship between Hazards, Accidents and their management through setting and meeting Safety Requirements could be included within the Hazard Log. However, if it is not sufficiently robust or well-structured, this may overload the Hazard Log and obscure the identification and clearance of Hazards. The requirements of this clause are an important part in demonstrating the robustness of evidence of safety and should be clearly documented and referenced.

11.2.10.2.

If hazards are not well defined when they are entered into the Hazard Log, then the rigour enforced by the

need for a clear audit trail of changes made, may make it very difficult to maintain the hazard and accident records in the most useful structure. An appropriate structure should therefore be designed and agreed before data entry starts.

11.2.11. Procedure Completion

11.2.11.1.

The Hazard Log ensures that a common set of information can be shared by all parties with a genuine need for access. A single Hazard Log should therefore be maintained that is accessible by all these parties.

11.2.11.2.

The Hazard Log may be run by the Prime Contractor or the MOD Delivery Team or a third party such as a Safety Assessment contractor. Indeed the Hazard Log may pass from one authority to another at key stages in the programme. For example, the Prime Contractor is likely to have greatest need of the Hazard Log during System Development, but the MOD Delivery Team may be a more appropriate controller when the System is in service.

11.2.11.3.

The Hazard Log should be under the control of a Hazard Log Administrator, who is responsible to the Prime Contractor's Project Safety Engineer or the MOD's Safety Manager. The Hazard Log Administrator should have full access to the Hazard Log allowing him to add, edit or close Hazards. All other personnel requiring access to the Hazard Log are allowed read only access. This allows for visibility of Hazards to all but the strict control and administration of hazards is limited to the Hazard Log Administrator.

11.3. Timing

11.3.1. Initial Production

11.3.1.1.

The Hazard Log should be established at the earliest stage of the programme and be maintained thereafter as a 'live' document or database to reflect the current design standard.

11.3.2. Review, Development and Acceptance

11.3.2.1.

A review of the Hazard Log is essential at regular intervals to ensure that Hazards are being successfully managed and that the robustness of the safety arguments in the Safety Case can be established.

11.4. Required Inputs

11.4.1. General

11.4.1.1.

This procedure for Hazard Log requires inputs from:

1. Outputs from Procedure SMP01 – Safety Initiation [2];
2. Outputs from Procedure SMP04 – Preliminary Hazard Identification and Analysis [3];
3. Outputs from Procedure SMP05 –Hazard Identification and Analysis [4];
4. Outputs from Procedure SMP06 –Risk Estimation [5];
5. Outputs from Procedure SMP07 –Risk and ALARP Evaluation [6];
6. Outputs from Procedure SMP08 –Risk Reduction [7];
7. Outputs from Procedure SMP09 –Risk Acceptance [8];
8. Outputs from Procedure SMP10 –Safety Requirements and Contracts [9].

11.4.1.2.

The Hazard Log is a database which references all the major items of Safety documentation relating to a project. This can include the following:

1. Safety Criteria Report;
2. Safety Requirements;
3. Hazard Identification Reports;
4. Hazard Analysis Reports;

5. Risk Analysis and Assessment Reports;
6. Safety Audit and Inspection Reports;
7. Safety Case Reports.

11.4.1.3.

The Hazard Log should store information on hazards, accidents and accident sequences which might be associated with the system. Thus it records the results of all the Risk Management procedures (SMP04 [10], SMP05 [11], SMP06 [12], SMP07 [13], SMP08 [14]and SMP09 [15]).

11.4.2. Supporting Documentation

11.4.2.1.

Where the Hazard Log has adequate capacity and resources permit, the following supporting documentation should also be either directly embedded or cross-referenced by hypertext link where the Log is an electronic format:

1. Material/system survey reports;
2. Design defect reports, concessions and production permits;
3. System/equipment breakdown and failure reports;
4. Reports of technical design/material state reviews;
5. Reports of quality, reliability and safety audits;
6. Accident and incident reports, during construction, maintenance or in-service operation.

11.4.2.2.

Hazard Log Reports will be produced for the purpose of review e.g. by the Project Safety Committee or the Independent Safety Auditor or communication of the current status of the Safety Programme. Where a computer tool is used to implement the Hazard Log, it should be capable of producing a range of reports, from detailed to summary.

11.4.2.3.

Since a Hazard Log is a structured way of storing and referencing data and records on Hazards, documenting the Risk Evaluation and other information relating to an equipment or system, clear cross-referencing to supporting documents is essential. The supporting documentation should be either directly embedded or cross-referenced by the Hazard Log.

11.5. Required Outputs

11.5.0.1.

Hazard Log Reports will be capable of showing the linkages between hazards, accidents and controls (i.e. which hazards could lead to which potential accidents, possibly with many-to-many relationships, and which controls relate to which hazards and accidents). They shall also differentiate between controls which are already in place and those which are being considered or planned.

11.5.0.2.

A Hazard Log should be used and maintained as the principal means of establishing progress on resolving risks associated with identified hazards. It will provide traceability of the hazard management process to show how safety issues are being dealt with and resolved.

11.5.1. Hazard Log Report

11.5.1.1.

The Hazard Log should be a continuously evolving record (database or document) which should stay with the system throughout its life cycle. A Hazard Log Report is a snap shot of the Hazard Log status on a given date.

11.5.1.2.

Hazard Log Reports will be produced for the purpose of review (e.g. by the Project Safety Committee or the Independent Safety Auditor or communication of the current status of the Safety Programme. Where a computer tool is used to implement the Hazard Log, it should be capable of producing a range of reports, from detailed to summary.

11.5.1.3.

Hazard Log Reports should be capable of showing the linkages between Hazards, Accidents and Controls (i.e. which hazards could lead to which potential accidents, possibly with many-to-many relationships, and which controls relate to which hazards and accidents). They should also differentiate between controls which are already in place and those which are being considered or planned.

11.5.2. Hazard Log Software

11.5.2.1.

The DE&S mandated corporate Hazard Log Tool is the Cassandra database system and its online equivalent, eCassandra. Team leaders should consider tailoring this system to meet their needs. DTs wishing to use an alternative Hazard Log Tool must be able to demonstrate that the proposed Alternative Acceptable Means of Compliance offers the same level of information/granularity so that visual representation and appropriate audit trail can be clarified and justified against the envisaged accident sequence in comparison to the mandated eCassandra tool.

11.5.2.2.

Whatever Hazard Log tool is adopted should be under strict configuration control to ensure robust audit trail.

11.5.2.3.

Cassandra is a Hazard Management System designed to meet the requirements of Def Stan 00-056 [1] and most other recognised safety management and assessment processes. In addition to recording information about hazards and accidents, risk classification and control measures, required in the conventional Hazard Log, Cassandra also enables hazards and accidents to be linked to show their relationships (one-to-many and many-to-many).

11.6. Annex A

11.6.1. Hazard Log Contents

11.6.1.1.

A suggested Hazard Log structure is as follows:

11.6.1.2.

Part 1 - Introduction

This part should describe the purpose of the Hazard Log, and indicate the environment and safety criteria to which the system safety characteristics relate. The following details, appropriate to the programme phase, should be contained in this part:

1. The purpose and structure of the Hazard Log. This should be of sufficient detail to ensure that all project staff understand the aim and purpose of the Hazard Log. The procedure for managing the Hazard Log should also be included;
2. A description of the system and its scope of use. This should include reference to a unique system identifier;
3. Reference to the system safety requirements;
4. The accident severity categories, probability categories, equivalent numerical probabilities and accident risk classification scheme for the system;
5. The design rules and techniques for each Safety Integrity Level;
6. The apportionment of the random and systematic (Safety Integrity Level) elements of the hazard probability targets between all the functions of the system (refer to publication “Acquisition Guidance on the Assurance of Safety in Systems Containing Complex Electronic Systems” for further information).

The description and scope of use of the system will be stated in order to indicate the environment to which the system safety characteristics relate. This information should be entered in Part 1 of the Hazard Log.

11.6.1.3.

Part 2 - Accident data

This part should give sufficient information to identify the accident sequence linking each accident and the hazards which cause it. It will include the following:

1. A unique reference;
2. A brief description of the accident ;
3. The accident severity category and probability targets appropriate to Risk Classes B and C;

4. A cross reference to the full description and analysis of the accident sequence in the safety programme reports. This information should be used to justify the subsequent setting of the hazard probability targets;
5. A list of the hazards and associated accident sequences that can cause the accident.

11.6.1.4.

Part 3 - Hazard data

This part should give sufficient information to identify the risk reduction process applicable to a particular hazard. A summary of all the hazards and their status, including any outstanding corrective action, should be contained within this part to provide an overview of the current situation. This part should contain the following information for each hazard:

1. A unique reference. A brief description of the Hazard which should comprise the functions or components and their states that represent the Hazard. Reference should also be made to the design documentation which describes the functions or components;
2. The related Accident severity category, and the random and systematic elements of the hazard probability targets appropriate to Risk Classes B and C;
3. The predicted probability for the random element of the Hazard;
4. A statement as to whether or not the hazard requires further action to reduce the risk from the system to a tolerable level;
5. A discussion of any possible means by which the risk could be reduced to a tolerable level, and notes on the re-evaluation of the Accident sequence following such action;
6. A brief description of the action to reduce risk, together with either a reference to the design documentation that has changed as a result of the action, or the justification for taking no action;
7. A cross-reference to the full description and analysis of the Hazard in the Hazard analysis reports.

11.6.1.5.

Part 4 - Statement of Risk Classification

A Statement of Risk Classification should be included to provide a brief statement of the current System Risk Class. It will contain sufficient information to enable it to be a standalone statement, and it should contain the Hazard Log reference to enable traceability to its supporting documentation.

11.6.1.6.

Part 5 – Journal

A journal should be constructed to provide a historical record of the compilation of the Hazard Log. It will contain the following information:

1. The date the Hazard Log was started;
2. Entries made in the Hazard Log, including any accident or hazard reference numbers;
3. Reference to the Safety Programme Plan;
4. References to analysis and assessment reports;
5. References to Safety Review and Project Safety Committee minutes.

11.7. Version Control

11.7.1. Version 2.3 to 3.0 Uplift

11.7.1.1.

Major uplift from the Acquisition System Guidance (ASG) to online version. POEMS has undergone major revision. Refer to the POEMS Transition Document for details.

11.7.2. Version 3.0 to 3.1 Uplift

11.7.2.1.

A minor uplift to correct spelling, grammar, and to remove some duplication of text.

11.7.3. Version 3.1 to 4.0 Uplift

11.7.3.1.

Major reorganisation of all SMPs:

- Restructure into a consistent format.
- Responsibilities, Alignment with Environment and guidance for different acquisition strategies have been removed and included in the POSMS summary.
- All further guidance has been placed into the Procedure section, and duplicated text has been removed
- Hazard Logs Content is detailed in Annex A

11.7.4. Version 4.0 to 4.1 Uplift

11.7.4.1.

Minor text changes to align with ASP taxonomy.

11.7.5. Version 4.1 to 4.2 Uplift

11.7.5.1.

Minor amendment to replace reference to Initial Gate and Main Gate and change these to Strategic Outline case, Outline Business Case and Full Business Case. This change brings terminology in line with JSP 655.

11.7.6. Version 4.2 to 4.3 Uplift

11.7.6.1.

Update to clarify eCassandra as the mandated Hazard Log Tool.

Source URL:https://test.asems.mod.uk/guidance/posms/smp11

Links
[1] https://test.asems.mod.uk/ExtReferences [2] https://www.asems.mod.uk/guidance/posms/smp01 [3] https://www.asems.mod.uk/guidance/posms/smp04 [4] https://www.asems.mod.uk/guidance/posms/smp05 [5] https://www.asems.mod.uk/guidance/posms/smp06 [6] https://www.asems.mod.uk/guidance/posms/smp07 [7] https://www.asems.mod.uk/guidance/posms/smp08 [8] https://www.asems.mod.uk/guidance/posms/smp09 [9] https://www.asems.mod.uk/guidance/posms/smp10 [10] https://test.asems.mod.uk/guidance/posms/smp04 [11] https://test.asems.mod.uk/guidance/posms/smp05 [12] https://test.asems.mod.uk/guidance/posms/smp06 [13] https://test.asems.mod.uk/guidance/posms/smp07 [14] https://test.asems.mod.uk/guidance/posms/smp08 [15] https://test.asems.mod.uk/guidance/posms/smp09