AURC

AUSTRALIAN UNIVERSITIES ROCKET COMPETITION

2024 AURC Hazard Log Guidance Note

Version 1.0: 11th March 2024

AYAA

Table of Contents

List of Figures

Revision History

Revision	Description	Date
Version 1.0	Initial Release	11/03/2024

1 Safety Theory

There are several theories and methodologies that attempt to categorise risk identification and management. While there are many valid and useful models available, this guidance note will elaborate on the Swiss Cheese Model and the Bowtie Model

1.1 Swiss Cheese Model

The Swiss Cheese model operates on the premise that controls (barriers) designed to prevent accidents occurring are never 100% effective.

The process of an accident occurring is visualised as an arrow traveling from a hazard source to an accident outcome, with the various barriers to the accident occurring modelled as obstacles. The nature of these barriers being imperfect is visualised as holes through which the accident cause can travel through, and as such these barriers resemble Swiss cheese (presented in Figure 1).

Key points to note include the necessity of multiple barriers to prevent accidents due to the inherent imperfection of controls. Even with multiple barriers present, accidents can still occur if there is a chain of failures (i.e. the holes line up). Additionally, the efficacy of controls can be represented through modelling – a decrease in control effectiveness (due to inadequate implementation or management) can be depicted by a barrier layer having more holes.

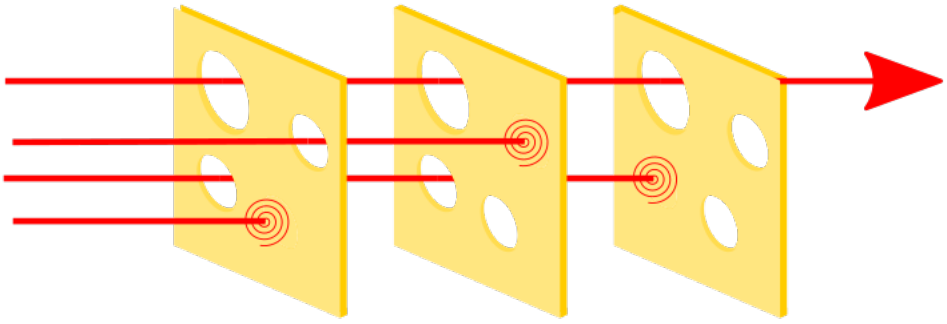

Figure 1: Visualisation of the Swiss Cheese Model [1].

1.2 Bowtie Model

The Bowtie model expands on the Swiss Cheese model by illustrating the relationship between causes, controls, outcomes, mishaps, and hazards. On the left side of the diagram, the various causes of the mishap are listed along with any preventative controls associated with them. The centre of the model is the mishap linked with the hazard which causes the critical event. This event could be an injury, or a loss of control of a hazardous situation. After the critical event occurs, only mitigative controls can reduce the severity of the outcomes, which are placed on the right of the diagram.

An example of a Bowtie diagram is presented in Figure 2.

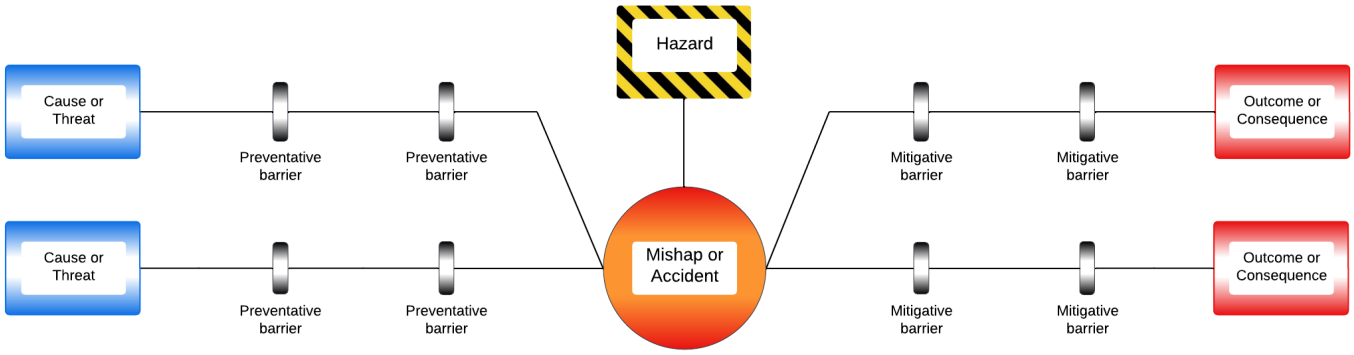

Figure 2: Example Bowtie diagram depicting the various elements used.

2 Definitions

2.1 Hazard

A hazard is generally defined as a source of potential harm to a person.

Identifying hazards has historically been driven by process engineering projects identifying sources of potentially harmful energy that could interact with personnel, such as mechanical, electrical, chemical or potential [2].

Outside of a process safety context, hazards have been identified by examining the potential harm arising from the loss of control of a situation. Examples of these are a loss of situational awareness or control of an aircraft.

It is important to note that there is a difference between loss of control (situational command) versus failure of a control (risk reduction). A loss of control itself isn't a hazard; controls are put in place specifically to mitigate the risks associated with hazards.

2.2 Mishap

A mishap (or accident) is defined as an event whereby a person is exposed to a hazard resulting in an injury.

2.3 Likelihood

The likelihood (in terms of risk) is the probability for the risk or mishap to occur. It is typically linked to a particular consequence level, as usually more minor outcomes are more likely to occur (e.g. minor injuries from tripping are far more likely than a broken bone). Note that this trend does not always apply; some types of incidents (typically high energy, e.g. explosions) will have the same likelihood for several outcomes, where the likelihood of minor injuries may be the same as a serious injury or fatality.

The Defence Safety Manual - Section 8 describes the various activity based likelihoods as follows [3]:

1. Almost Certain: Expected to occur during the planned activity. Is known to occur frequently in similar activities.
2. Probable: Expected to occur in most circumstances but is not certain. Is known to have occurred previously in similar activities.
3. Occasional: Not expected to occur during the planned activity. Sporadic but not uncommon.
4. Improbable: Not expected to occur during the planned activity. Occurrence conceivable but considered uncommon.

5. Rare: Not expected to occur during the planned activity. Occurrence conceivable but considered highly unlikely / an exception not expected to occur.

It is possible for likelihoods to be categorised as a percentage chance of occurring; this is called a quantitative likelihood. Although these can be very effective in helping manage risk, they require extensive testing or research to gain knowledge of the statistical failure rates of the various parts of the system. This level of rigour will not be required for the AURC.

2.4 Consequence

The consequence (in terms of risk) is the severity of harm that could eventuate if an accident occurs. A useful way to categorise outcomes is based on the level of care required to manage the outcome.

The Defence Safety Manual - Section 8 defines the various levels of consequences as follows [3]:

1. Catastrophic: Multiple fatalities or 10 or more injuries/illnesses categorized as critical.
2. Critical: Single fatality and/or permanent total disability or 10 or more injuries or illnesses categorized as major.
3. Major: Serious injury or illness of a person, requiring immediate admission to hospital as an inpatient and/or permanent partial disability or 10 or more injuries/illness categorized as moderate.
4. Moderate: Injury or illness causing no permanent disability, which require non-emergency medical attention by a registered health practitioner, or 10 or more injuries or illnesses categorized as minor.
5. Minor: Minor injury or illness that is treated in the workplace (first aid) or by a registered health practitioner, with no follow up treatment required.

2.5 Risk

Risk is simply the combination of the consequence and likelihood of an outcome. Some fields such as process engineering also consider exposure – the number of people and amount of time spent exposed to a risk – in addition to the consequence and likelihood.

The nature of risk is multiplicative between the consequence and likelihood: situations with serious outcomes that are very unlikely can be given a similar weighting to situations with very minor outcomes that are expected to occur frequently. High consequence, high likelihood events are generally considered unacceptable, and low consequence, low likelihood events usually are well within a group's risk appetite.

Qualitative risk assessments are generally done using risk matrices. These have the consequence and likelihood on neighbouring sides of a matrix, with the correlating risk values populating the matrix. The dimensions of a matrix depend on the number of categories used to define the consequence and likelihood.

The Defence Safety Manual - Section 8 uses the risk matrix presented in Figure 3.

Defence Work Health & Safety Risk Matrix

Likelihood descriptors \ Consequence descriptors		Minor (A)	Moderate (B)	Major (C)	Critical (D)	Catastrophic (E)
		Minor injury or illness that is treatable in the workplace (first aid) **OR** by a registered health practitioner, with no follow up treatment required.	Injury or illness causing no permanent disability, which requires non-emergency medical attention by a registered health practitioner **OR** 10 or more injuries or illnesses categorised as 'minor'.	Serious injury or illness requiring immediate admission to hospital as an inpatient and/or permanent partial disability **OR** 10 or more injuries/illnesses categorised as 'moderate'.	Single fatality and / or permanent total disability **OR** 10 or more injuries or illnesses categorized as 'major'.	Multiple fatalities **OR** 10 or more injuries / illnesses categorised as 'critical'.
Almost certain (5)	**Activity:** Expected to occur during the planned activity. Is known to occur frequently in similar activities. **System:** Expected to occur several times a year or often during the system life-cycle. Is known to occur frequently in similar systems being used in the same role and operating environment.	**(A5) LOW**	**(B5) MEDIUM**	**(C5) HIGH**	**(D5) VERY HIGH**	**(E5) VERY HIGH**
Probable (4)	**Activity:** Expected to occur in most circumstances, but is not certain. Is known to have occurred previously in similar activities. **System:** Expected to occur one or more times per year or several times in the system life cycle. Is known to occur previously but is not certain to occur.	**(A4) LOW**	**(B4) MEDIUM**	**(C4) HIGH**	**(D4) HIGH**	**(E4) VERY HIGH**
Occasional (3)	**Activity:** Not expected to occur during the planned activity. Sporadic but not uncommon. **System:** Expected to occur less than once per year or infrequently during system life cycle.	**(A3) VERY LOW**	**(B3) LOW**	**(C3) MEDIUM**	**(D3) HIGH**	**(E3) HIGH**
Improbable (2)	**Activity:** Not expected to occur during the planned activity. Occurrence conceivable but considered uncommon. **System:** Not expected to occur, but possible to experience one or more events during the system life cycle.	**(A2) VERY LOW**	**(B2) VERY LOW**	**(C2) LOW**	**(D2) MEDIUM**	**(E2) MEDIUM**
Rare (1)	**Activity:** Not expected to occur during the planned activity. Occurrence conceivable but not expected to occur. **System:** Only expected to occur in rare or exceptional circumstances or no more than once during the system life cycle.	**(A1) VERY LOW**	**(B1) VERY LOW**	**(C1) VERY LOW**	**(D1) LOW**	**(E1) LOW**

Figure 3: Defence WHS Risk Matrix [2].

2.6 Controls

A control is any system, method or action that reduces the risk of a mishap. A control can be preventative or mitigative. Preventative controls aim to prevent an accident occurring, and mitigative controls aim to reduce the severity of accident after it has occurred. Examples can be a safety briefing (preventative) versus an evacuation plan and first aid (mitigative).

The Defence Safety Manual - Section 8 defines the various levels of controls as follows [3]:

1. Eliminate – the most effective control measure involves elimination of the hazard. Eliminating the hazard will also eliminate any risks associated with the hazard. Eliminating hazards is often more cost effective and practical to achieve at the design or planning stage of a platform, product, process or activity;
2. Substitute – involves replacing the hazard with a hazard that has a lower level of risk (e.g. substituting a solvent-based paint with a water-based product, using an Unmanned Aerial Vehicle (UAV) instead of a manned aircraft);
3. Isolate - involves isolating the hazard by physically separating the source of harm from people by using distance or barriers (e.g. installing guarding on machinery or barriers to prevent access);

4. Engineering – are controls that are physical in nature, such as a mechanical device or process (e.g. mechanical isolation - mechanical lockouts or tag-outs or software systems that provide redundancies);
5. Administrative – are work methods or procedures that are designed to minimise exposure to a hazard (e.g. procedures on how to operate machinery safely, limiting the exposure time to a hazardous task, use of safety signs to warn people of a hazard); and
6. Personal Protective Equipment (PPE) – personal protective equipment limits the exposure to harmful effects of a hazard (e.g. gloves, respirators, glasses, coveralls, hearing protection, hard hats).

Controls are categorised into a hierarchy based on their effectiveness at reducing risks. This hierarchy is presented in Figure 4. Elimination is the only level of control that can completely remove the risk of an accident, but in practice this is very difficult to achieve. Where feasible, higher level (more effective) controls should be used before relying on lower level controls (i.e. attempt to apply engineering controls before applying administrative controls). PPE should never be the sole level of control to reduce risk.

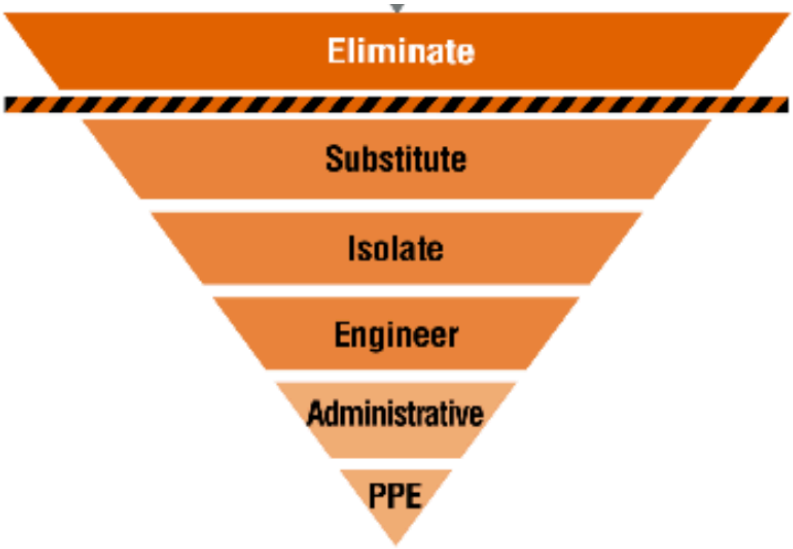

Figure 4: Hierarchy of controls [2].

3 Hazard Log Guidance

Please note that there are informative notes present on the headings in the hazard log. You can see these by mousing over cells in the hazard log that have a small red mark in the top right corner.

Entries into the hazard log that are given as an example are in grey, and you are encouraged to develop more than what is given as an example. You are also free to remove or replace the given examples with entries more appropriate to your risk assessment.

3.1 Mishap

Mishaps are not a strictly defined set of incidents but are generally created by identifying the nature of similar hazards and controls. Some mishaps are very widespread and common across many industries, such as fire and noise, however some might be more specific to a particular field, such as maritime or aerospace.

You are encouraged to create more mishaps in the risk register as you undertake your risk analysis. The mishaps given as examples should be considered, but you should also be able to identify further possible mishaps.

Mishaps can have many causes and outcomes.

3.2 Causes

Causes are a series or chain of events that can lead to a mishap. They are also known as "threats". Causes are where preventative controls need to be applied. Additionally, the hazards associated with a chain of events that could cause a mishap should be assigned to the relevant cause.

The failure of a control cannot be a cause of an accident (i.e. the failure of a car's emergency braking system cannot be considered a cause of an accident).

A cause can have multiple preventative controls and hazards assigned to it.

3.3 Outcomes

Outcomes are the descriptive consequences of a failure to prevent a mishap from occurring. Each outcome will need to have any relevant mitigative controls assigned to it, and an associated risk assessment.

An outcome can have multiple mitigative controls, but only a single risk assessment assigned to it.

3.4 Risk Assessments

You will need to undertake a risk assessment on each type of outcome. You will need to evaluate an appropriate likelihood and consequence based upon the given descriptors for each assessment. Initial risk assessments assess the risk of the mishap before the controls are applied; residual risk assessments take place after the controls are applied.

The difference between the risk assessments should demonstrate the effectiveness you believe the controls have on the given outcome. A control generally reduces the likelihood of the event taking place, however some controls can reduce the consequence – you must be able to justify your risk assessments.

The "most limiting" or "driving" factor of a mishap is the outcome, cause(s) and hazard(s) that give the highest risk rating. When hazard ratings are tied, preference is given to the rating that has a more severe outcome. Efforts should be focused on reducing the most limiting risk as far as reasonably practicable.

3.5 Hazards

Hazard should populate the hazards list and be assigned to relevant causes. These hazards can be created using the provided basic hazard identification worksheet, but you are free to use other types of hazard identification techniques.

Hazards need to have their associated system state assigned to them.

Please ensure and cross-check that all active hazards present in the hazard list are used in the risk register, and that any hazard code used in the risk register has the correct hazard present in the hazard list.

Identity and document control will assist in avoiding errors or duplicates – if a hazard is retired or no longer in use in any way, it is recommended to keep the out-of-use hazard ID and make a note in the hazard list why that hazard is no longer in use.

3.6 Controls

Implemented or planned controls should populate the controls list and the relevant columns in the risk register. The controls in the controls list need to include information on their position on the controls hierarchy and whether they are mitigative or preventative.

Preventative controls must be assigned to Causes, and mitigative controls must be assigned to Outcomes.

For all controls that are assigned to a cause or outcome in a mishap, please fill out their details in the "Controls" column of the Risk Register. This will assist in providing easy to find information of the various controls assigned to the mishap.

Please undertake the same cross-checking and identity controls as hazards, there should be no unassigned controls in the controls list, and no controls should be in the risk register without their corresponding details in the controls list.

4 References

[1] Wikipedia, "Swiss cheese model," [Online]. Available: https://en.wikipedia.org/wiki/Swiss_cheese_model. [Accessed 2024 March 10].

[2] Defence Australia, Work Health and Safety Branch, "SafetyMan - Section 8 - Risk Identification and Management," [Online]. Available: https://www.defence.gov.au/about/governance/work-health-safety/policy. [Accessed 10 March 2024].

[3] "Energy," 10 March 2024. [Online]. Available: https://en.wikipedia.org/wiki/Energy#Forms.

THANK YOU

AYAA would like to express our thanks to you for competing in the 2024 Australian Universities Rocketry Competition. With your help, we can continue to strengthen the Australian space sector and provide industry relevant extracurricular experience to undergraduate and postgraduate university students of all STEM disciplines. Please do not hesitate to direct any questions about the AURC to aurc@ayaa.com.au or reach out to our team on the Slack channel.