EFFECTIVE BOWTIE DIAGRAM DEVELOPMENT – SUPPORTING SAFETY AND RISK MANAGEMENT

Steven Gibson[1], Kate Harding[2],

[1]*ESR Consulting,* [2]*KVH Consulting,*

Corresponding Author: steve.esr.consulting@gmail.com

SUMMARY

Bowtie diagrams have been utilised for some years as relatively simple aides to understanding and communicating safety hazards. However, the simple structure of the Bowtie diagram belies the complexity in developing models beyond the text-book examples, particularly at the system level where there may be many inter-related hazard scenarios.

In this paper, the authors draw on many years' experience developing risk models to share practical techniques for developing logical, structured and robust Bowtie diagrams to effectively characterise accident scenarios: their causes, potential consequences, and those control measures designed to prevent or minimize the risk.

Some of the pitfalls and how to identify them are discussed, including:

- Bowtie terminology and its relationship to common risk management elements.
- The distinction between hazards and Bowtie 'top events'.
- Effective top event selection and why this matters.
- Consideration of the relationship between Bowtie top events, direct threats and consequences in more complex event sequences.
- Enabling and causal event identification, and how distinguishing these from risk control failures leads to a better understanding of risk.
- Effective identification of independent risk controls, and why more is not necessarily better.

Drawing on examples from real-world railway systems, application of the Bowtie diagram technique is demonstrated, and concludes with a brief overview of available software tools and open-source options.

1 INTRODUCTION

The use of the Bowtie diagram as a hazard assessment methodology dates to at least the early-1980s in the process industry, and since the 1990s has seen widespread use alongside techniques such as Layers of Protection Analysis (LOPA), Fault-Tree Analysis (FTA) and Event-Tree Analysis (ETA). In more recent years the use of the Bowtie diagram methodology has become more common in other high-risk industries such as aviation and railways.

Unlike LOPA, FTA, ETA and similar quantitative and semi-quantitative techniques, the structured diagrammatic nature of the Bowtie diagram provides a more readily understandable visualisation of hazard scenarios: the relationships between the causes of hazardous events, the potential consequences of these events, the control measures (barriers) preventing the event from occurring, and those barriers in place intended to minimise the potential consequences.

The Bowtie diagram is particularly useful in enabling communication of hazard scenarios with the wider workforce in a more effective and engaging manner (compared to say a hazard register), and provides a direct link between technical and other control measures and elements of the Safety Management System (SMS), Safety Critical Systems and Safety Critical Tasks, for example.

Conventionally, the Bowtie diagram comprises: a *Hazard*, a *Top Event*, one or more *Consequences*, one or more *Threats*, preventative *Barriers*, and mitigative *Barriers* [1]. The diagram is drawn with the *Hazard* and *Top Event* depicted in the centre, with *Threats* on the left of the *Top Event*, and *Consequences* on the right. *Barriers* are preventative where positioned between a *Threat* and the *Top Event*; and mitigative between the *Top Event* and a *Consequence*.

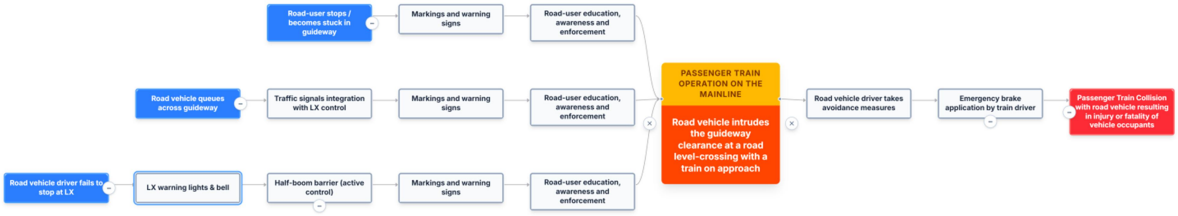

Figure 1: The Bowtie Diagram

More advanced aspects such as *Escalation Factors* and linking *Top Events* are discussed in Section 5. An example Bowtie diagram is illustrated in Figure 1.

2 NOMENCLATURE

The following key terms and their definitions are used in this paper, these are discussed in Section 3.

Accident – an unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage. (EN 50126-1:2017)

(Safety) Barrier – physical or non-physical means, which reduces the frequency of a hazard and/or a likely accident arising from the hazard and/or mitigates the severity of likely accidents arising from the hazard. (EN 50126-1:2017)

Causal Factor – a necessary and sufficient condition which can result in the *hazardous state*.

Critical Event – a *hazardous state.*

Escalation Factor – a condition, event, or failure that reduces the effectiveness of a *safety barrier*.

Hazard – a condition that could lead to an *accident*. (EN 50126-1:2017)

Hazardous State – a state that has the potential to cause harm to persons, significant material damage or other unacceptable consequences. (IEC 60050-192)

Initiating Mechanism – a necessary condition which can result in the *hazardous state*.

Mishap – an unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment. Accident. (MIL-STD-882c)

Top Event – a *hazardous state*, often articulated as a loss-of-control.

3 HAZARDS, HARM AND CRITICAL EVENTS

Risk assessment and hazard control are the primary safety-related activities that are needed to ensure an acceptable level of safety for a system: fundamental to these activities is *hazard identification.*

EN 50126-1:2017 [2] defines a *hazard* as: condition that could lead to an *accident*. Furthermore, an *accident* is defined “unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage”. This definition is consistent with MIL-STD-882c [3] which defines a *hazard* as: a condition that is prerequisite to a mishap. And *mishap* as “an unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment. Accident”.

In both EN 50126-1:2017 and MIL-STD-882c a *hazard* is described as a condition.

Other comparable standards offer a range of definitions:

potential source of harm (IEC 61508-4:2010 [4])

a physical situation with a potential for human injury (EN 50126-1:1999 [5])

a condition that could lead to an accident (EN 50129:2018 [6])

potential source of harm (IEC 60050-903:2013 [7])

It is interesting to note that EN 50126-2:2007 [8] states under the definition of *hazard*: “the limitation of hazards to physical situations might be rather restrictive in some cases. Therefore, the following definition, as given in EN 50129, is considered more appropriate: a condition that could lead to an accident”.

While in theory identifying hazards systematically should be straightforward, in practice the basic concept of what comprises a hazard can be difficult to define, and hard to distinguish from causal factors and consequences.

Ericson in *Hazard Analysis Techniques for System Safety* [9] expands on the description of the hazard as a condition, by describing a hazard and accident as the same entity: only the state has transitioned from a potential event to an actual event. He characterises the hazard as comprised of three basic components necessary for the hazard to exist: the *Hazard Element* (source), the *Initiating Mechanism* (mechanism), and *Exposed Group* (those with the potential for harm), as illustrated in Figure 2.

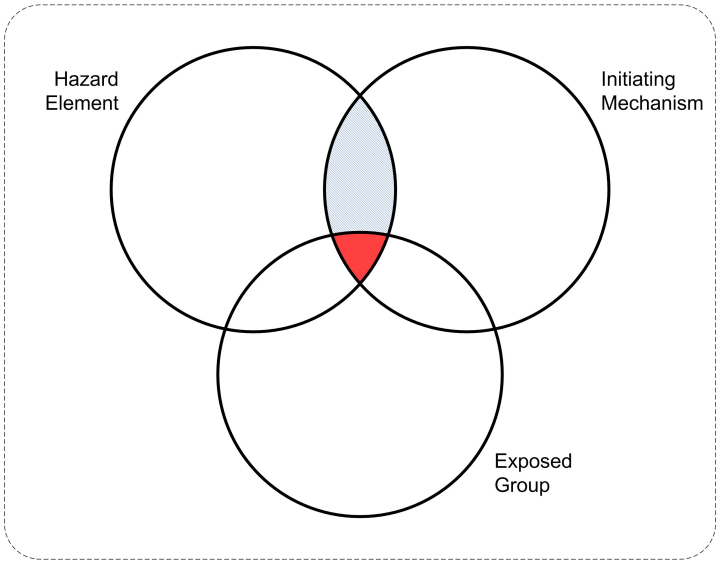

Figure 2: Hazard 3-tuple

For the example at Figure 1: the *hazard element* is the train’s kinetic energy, the *initiating mechanism* being the train’s approach to the level-crossing and the road vehicle intruding into the guideway, and the *exposed group* being those personnel exposed to the potential harm.

In conventional Bowtie diagram construction, the central *Top Event* is often described as a loss-of-control condition. In comparison to the definition of *hazard* (EN 50126-1:2017) and *hazardous state* (IEC 60050-192), there is no significant differentiation between the three terms.

In *The cause-consequence diagram method as a basis for quantitative accident analysis* [10] Nielson presented a method of which the main principle involves the concept of a critical event used to combine the logical connections between the causes of the critical event and the possible consequences of it. In Bowtie diagram construction, the authors prefer the term *critical event* to better convey the intent of the central element of the Bowtie diagram, instead of the ineffable *Top Event*.

The *critical event* is the intersection of the *hazard element* and *initiating mechanism* (blue shading in Figure 2) – this is the *hazardous state* with potential to cause harm. The intersection of the *critical event* and *exposed group* is the *hazard* (shown in red).

The hazard diagram illustrates that a *hazard* consists of three essential and necessary components: these three components are required for the *hazard* to exist. If one of the three elements is removed, then the *hazard* is eliminated. If one or more of the elements is reduced (frequency of occurrence for example) then the risk of the *accident* is reduced.

In the example of level-crossing operation in a suburban network: reducing the frequency of services reduces the exposure to the hazard source (being the train's kinetic energy); reducing the train's approach speed reduces the severity of the potential *accident*; and reducing the frequency of road vehicles crossing reduces the frequency of the initiating event. While grade separation doesn't remove the source of the hazard in this case, it does eliminate the initiating mechanism (road vehicle intruding into the guideway at a level-crossing).

The potential difficulty in articulating *hazards* and distinguishing these from *hazardous states*, *causal factors* and *accidents* is compounded by the conventional Bowtie terminology of Hazard, Top Event, Threat, and Consequence – in the following sections, the *hazard* and *critical event* concepts explored here are applied in the context of developing more effective Bowtie diagrams.

4 THE BOWTIE HAZARD MODEL

In the context of a Bowtie diagram, Figure 3 illustrates the relationship between the h*azard element*, c*ritical event*, *initiating mechanism* and e*xposed group.*

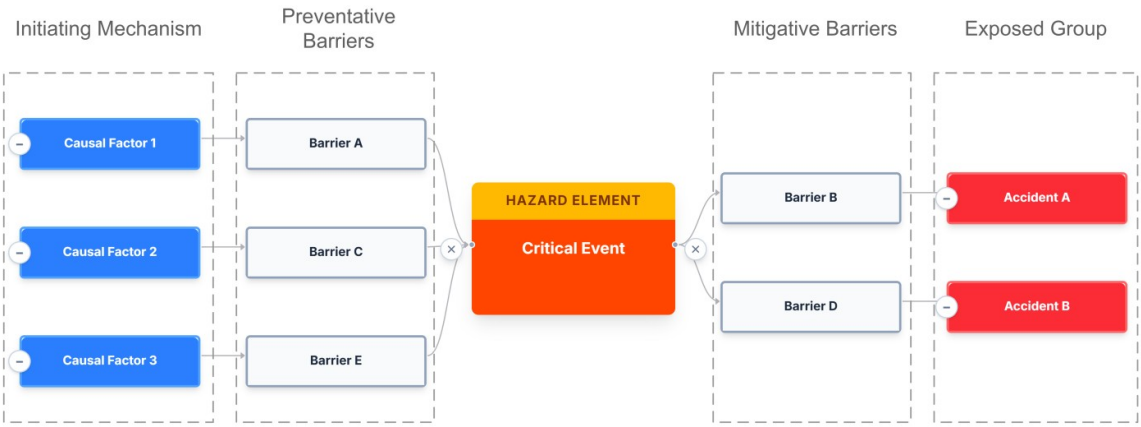

Figure 3: The Bowtie Hazard Model

In common with all forms of all hazard analyses, the initial step for developing a Bowtie model is to identify all hazards for the system under consideration followed by considering credible *accident* outcomes. Once this is complete, a backwards search from the *critical event* is conducted to identify the causal mechanisms, and finally preventative and mitigative safety *barriers* are identified to reduce the risk to a level which is as low as is reasonably practicable.

4.1 Hazard Identification

When conducting a preliminary search for hazards, the concept of the hazard 3-tuple (Figure 2) provides a useful model against which proposed hazards can be gauged in the context of the system.

The h*azard element* describes a potentially harmful source, substance, process or activity. For most engineered systems, *hazard elements* can be identified through a checklist search (for example iESM [11] and Safe Work Australia [12]).

In assessing a proposed *hazard element* for inclusion, if eliminating the *hazard element* does not eliminate the *accident* risk then this is not a true hazard source. For example, a failed lineside signal is a dangerous failure but not a *hazard element* – removing the failure of the lineside signal does not eliminate the *accident* risk (refer Table 1), it merely decreases the risk and is therefore a control.

In articulating the *hazard element*, consideration should be made to the operating context, for example, hazards associated with rolling stock kinetic energy will differ in the context of passenger train operation, freight train operation, both on the mainline and in the stabling yard.

In the search for hazards, the analyst should be careful to consider all potential operating modes, not just 'normal business' – recovery of a failed train for example may present a range of unique hazards.

Some well-described and not so well-described, examples are provided in Table 1.

Table 1: Examples of Hazard Elements

Hazard Element	Comment
Driving a passenger train on the mainline.	Passenger services are normal operation with the potential for a loss of control of kinetic energy.
Energised high-voltage Overhead Line Equipment (OLE).	The OLE is a source of high-voltage and high-current energy.
Working at height (> 2 m).	Working at height is an activity which exposes the worker to potential energy (i.e. an uncontrolled fall from height).
Passenger train exceeds permissible speed for track section.	This can be a dangerous condition but is not a *hazard element*. This could be an *initiating mechanism* or a failure of a *barrier*, depending on the context.
Signal passed at danger.	This is an *causal factor* or a failure of a *barrier* and not a *hazard element*. Eliminating the signal doesn't eliminate the hazard.
Lineside signal failure.	This is certainly a dangerous failure but is not a *hazard element*. This could be a *causal factor* or a failure of a *barrier*, depending on the context.

4.2 Articulating the Critical Event

The *critical event* is the hazardous state that could lead to an *accident*. In the process industry this state is commonly described as the point at which control over the hazard, or its containment, is lost,

Selecting a suitable *critical event* may be reasonably straight forward, particularly for scenarios which can be directly described in terms of a loss of control, loss of containment, loss of separation, or loss of stability that evidently leads to an obvious *accident*.

In other cases, the choice for the *critical event* may be less obvious. For example, there is no doubt that a significant train over-speed event can result in a derailment, and is commonly described as 'an *accident'*: in this case is the derailment the *critical event* or the *accident?* Here the derailment is the loss of control of the train's kinetic energy at the rail-wheel interface: it's the *critical event*, with over-speed being one causal factor. For the same reasons, driving a car too fast for a given road condition is not the *critical event*: the *critical event* is a loss of road surface – tyre adhesion. However, a loss of separation between a train and an obstacle (the *critical event*) can result in a collision (the *accident*), which may subsequently cause derailment (refer to Figure 5).

In articulating the *critical event*, the analyst should be careful to consider if the scenario is too broad, perhaps leading to a diagram of unmanageable size, or too narrow, requiring multiple diagrams. One technique to assist in managing this is provided in Section 5. In addition, where the scope is too broad, specific *barriers* may not be appropriate for all circumstances. For example in an overspeed scenario, passenger rolling stock may be provided with Automatic Train Protection (ATP) devices; these however may not be fitted to all classes of rolling stock in the scope of the Bowtie study.

Some well-described examples and counter examples are provided in Table 2 and Table 3.

Table 2: Well-described Examples of Critical Events

Hazard Element	Initiating Mechanism	Critical Event	Comment
Driving a passenger train on the mainline.	Vehicle intruding the guideway, and the train on approach to the level-crossing.	Road vehicle intrudes the guideway clearance at a road level-crossing with a train on approach.	This describes a loss of separation between the train and a road vehicle.

Driving a passenger train on the mainline.	Obstacle intruding the guideway, and the train on approach.	Loss of separation between the obstacle and train.	This describes a loss of separation between the train and obstacle.
Driving a passenger train on the mainline.	Rail-mounted vehicle (RMV) in a following track section.	Loss of separation between passenger train and rail-mounted vehicle.	This describes a loss of separation between the train and another RMV.
Driving a passenger train on the mainline.	Passenger train exceeds safe speed for track section.	Passenger train derailment - loss of control over the train's wheel-rail interface.	This describes a loss of control over the train's wheel-rail interface.
Energised high-voltage Overhead Line Equipment.	Maintenance activity adjacent to OLE equipment.	Maintenance activity adjacent to OLE equipment resulting in arc flash.	This describes personnel exposure to a high-voltage source of energy.

Table 3: Counter Examples of Critical Events

Hazard Element	Initiating Mechanism	Critical Event	Comment
Energised high-voltage Overhead Line Equipment.	Maintenance activity adjacent to OLE equipment.	Failure to isolate OLE equipment.	This is the failure of a *barrier* (isolation) and is not a *critical event*.
Driving a passenger train on the mainline.	Lineside signal failure.	Signal passed at danger.	While a dangerous condition, these describe failures of a control (*barrier*). The *critical event* is a loss of separation between the passenger train and another RMV.

4.3 Identify Credible Accidents

Once the *critical event* has been defined the next step is to determine the credible consequences (*accidents*). This is generally preferable to exploring causal events first as 1) only those causal events which can lead to the defined *accidents* should be selected, and 2) often the Bowtie study is scoped to identify major *accident* events (potential *accidents* which exceed a specified level of harm).

The description of the *accident* should include the <accident event>, <actor> and <harm>. For example: "Collision with an obstruction resulting in driver injury". It is important to articulate the *accident* event, since different *barriers* may be required to mitigate potential harm depending on the specific event which leads to the harm. For example, "Fire at a station resulting in serious injury due to thermal radiation" could require different mitigation *barriers* than "Fire at a station resulting in serious injury due to smoke inhalation".

As a counter example, "Evacuation of the station due to fire" is not a well-described *accident* since the station would be evacuated as a result of the fire being detected – the evacuation is a *barrier* to mitigate escalation of the event, not the *accident* itself.

Accidents may also lead to causal events on other Bowties – for example a derailment on the mainline which obstructs the adjacent guideway may be an initiating event to a collision. This is revisited in Section 5.

4.4 Initiating Mechanisms and Causal Factors

Each *causal factor* is a specific instance of an *initiating mechanism* and should be sufficient, in conjunction with the *hazard element*, to directly lead to the *critical event* – the 3-tuple comprising a *causal factor*, *hazard element* and *exposed group* is necessary and sufficient to realise each *accident* for every *causal factor.*

If an individual c*ausal factor* can only realise the *hazardous state* in combination with one or more other *causal factors* (or some external event) then it is not sufficient and is incorrect. In addition, if an *accident* can only be realised by a sub-set of *causal factors*, then the Bowtie is incorrectly formulated and needs to be restructured.

A common error in developing Bowties is treating failure of a safety measure, or human factor elements as *causal factors*, in both cases these are more properly addressed *escalation factors* – these are discussed further in Section 5.

Table 4: Examples of Causal Factors

Causal Factors	Hazard Element	Critical Event	Comment
Road vehicle queues across guideway.	Driving a passenger train on the mainline.	Road vehicle intrudes the guideway clearance at a road level-crossing with a train on approach	The *causal factor* is a sufficient and credible condition to realise the *critical event* in combination with the *hazard element*.
Road vehicle driver fails to stop at the activated level-crossing (LX).	Driving a passenger train on the mainline.	Road vehicle intrudes the guideway clearance at a road level-crossing with a train on approach.	The *causal factor* is a sufficient and credible condition to realise the *critical event* in combination with the *hazard element*.
Broken rail.	Driving a passenger train on the mainline.	Passenger train derailment - loss of control over the train's wheel-rail interface.	The *causal factor* is a sufficient and credible condition to realise the *critical event* in combination with the *hazard element*.

Table 5: Counter Examples of Causal Factors

Causal Factors	Hazard Element	Critical Event	Comment
Failure of the LX active protection devices.	Driving a passenger train on the mainline.	Road vehicle intrudes the guideway clearance at a road level-crossing with a train on approach.	This is a failure of a safety system (*barrier*). While it may increase the likelihood of an *accident*, it is not a cause of the *critical event* on its own.

4.5 Preventative and Mitigative Barriers

Barriers are 'physical or non-physical means, which reduce the frequency of a hazard and/or a likely *accident* arising from the hazard and/or mitigates the severity of likely *accidents* arising from the hazard' (EN 50126-1:2017). A preventative *barrier* is one that prevents or reduces the likelihood of the *critical event* from occurring, *mitigative barriers* act after the *critical event* has occurred and prevents or reduces the severity of an *accident*.

Barriers can be hardware controls, relying on engineered systems; or human controls relying on the actions of people, including procedures and instructions, to carry out activities.

Each *barrier* should be effective, independent, and not rely on other controls to function.

Table 6: Examples of Barriers

Critical Event	Barrier	Comment
Road vehicle intrudes the guideway clearance at a road level-crossing with a train on approach.	Automatically activated LX warning bells and lights.	This is an example of a preventative *barrier*; the LX active warning system alerts vehicle drivers of an approaching train, indicating that they should stop short of the guideway.
Passenger train passes a signal at danger with a rail-mounted vehicle in the next section.	ATP application of emergency brake.	This is an example of a mitigative *barrier*; the brake application both reduces the likelihood of impact and the consequence of collision.
Road vehicle intrudes the guideway clearance at a road level-crossing with a train on approach.	Train driver has clear sight lines.	This is not a complete nor effective *mitigative barrier* in its own right. It is an effective *escalation barrier* which helps minimise the driver's braking reaction time.

5 EXTENDING THE BASIC BOWTIE MODEL

5.1 Escalation Factors and Barriers

An *escalation factor* is a condition that can reduce the effectiveness of the preventative or mitigative *barrier* to which it is attached – these do not directly cause the *critical event* or *accident*, however, they increase the likelihood of undesired consequences. An *escalation barrier* reduces the impact of the *escalation factor*. *Escalation factors* and *escalation barriers* are illustrated in Figure 4.

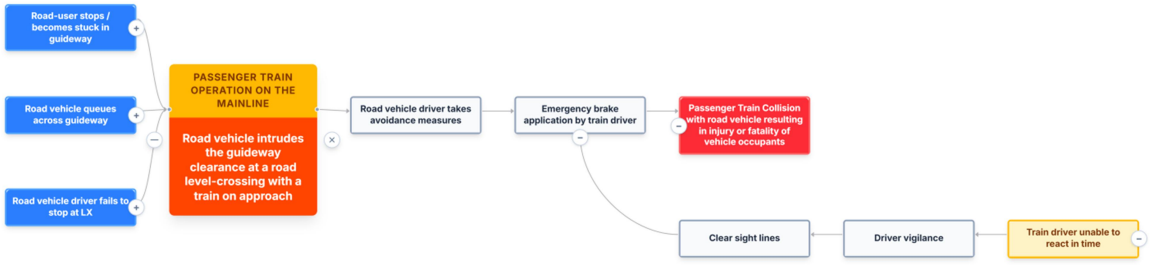

Figure 4: Escalation Factors

Avoiding a collision by the timely application of the train's emergency brake by the driver is one mitigating action. Models (such as the Australian Level Crossing Assessment Model [13]) identify reduced sight lines as a risk factor – this is not a complete nor effective mitigative *barrier* in its own right. However, it is an effective *escalation barrier* that helps minimise the driver's reaction time.

5.2 Linking Critical Events

Linking of critical events can be useful where the primary consequence of a *critical event* can escalate to a subsequent *critical event.* For example, a loss of separation of rolling stock (the *critical event*) could result in a collision (*accident*), this collision could subsequently result in the spill of flammable goods (the subsequent *critical event*) resulting in the collision escalating into a fire or explosion. Linking in this way provides the opportunity to consider those additional *barriers* which may prevent or minimise the risks associated with the initial *accident* escalating.

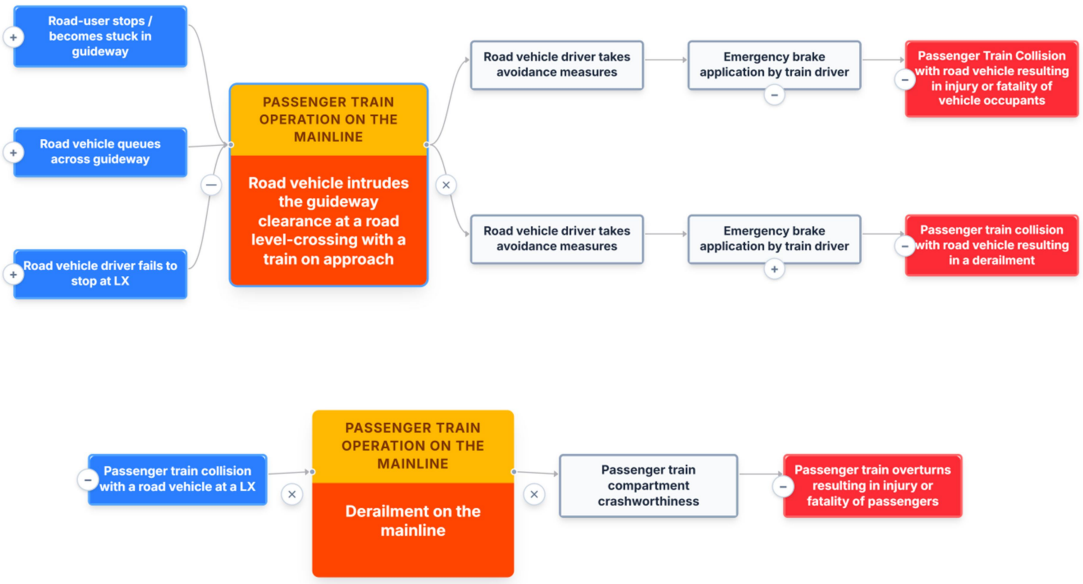

Figure 5: Bowtie Linking

6 TOOLS

For casual or infrequent use, general-purpose diagramming applications such as Visio and drawio can be used to develop Bowtie diagrams.

There are a number of commercial Bowtie software packages including BowTieXP and Synergi Life; these generally provide a large number of features supporting enterprise risk management, including: threat and barrier libraries, barrier classification, action management, and report generation.

Nexus Bowtie Builder (solsticeglobal.co.uk/nexus) supports the core Bowtie features and provides an alternate product to the enterprise-targeted solutions: the Bowtie diagrams in this paper have been created using Nexus Bowtie Builder.

7 CONCLUSIONS

Developing effective logical and structured Bowtie diagrams requires technical discipline to move beyond simplistic textbook examples. The paper demonstrates that a precise definition of what constitutes a hazard is fundamental to successful modelling. By applying the hazard 3-tuple concept, incorporating the hazard element, initiating mechanism, and exposed group, analysts can systematically identify hazards, their associated causal factors, and accident outcomes to ensure diagram integrity. Key findings highlight that barriers must be effective and independent, while distinguishing secondary escalation factors from initiating mechanisms. Furthermore, linking critical events provides a method for managing complex, cascading accident scenarios within high-risk industries.

Ultimately, these structured visual models provide a vital communication link between technical risk assessment and organisational safety management systems.

8 REFERENCES

[1] Bow Ties in Risk Management: A Concept Book for Process Safety, Center For Chemical Process Safety, 2018.

[2] CENELEC Standard EN 50126-1:2017 Railway applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process.

[3] Military Standard MIL-STD-882C System Safety Program Requirements, 1993.

[4] International Electrotechnical Commission Standard IEC 61508-4:2010 Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems – Part 4: Definitions and Abbreviations.

[5] CENELEC Standard EN 50126-1:1999 Railway applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Basic Requirements and Generic Process.

[6] CENELEC Standard EN 50129:2018 Railway applications - Communication, Signalling and Processing Systems - Safety Related Electronic Systems for Signalling.

[7] International Electrotechnical Commission Standard IEC 60050-903:2013 International Electrotechnical Vocabulary - Part 903: Risk assessment.

[8] CENELEC Standard EN 50126-2:2007 Railway applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Guide to the Application of EN 50126-1 for Safety.

[9] Ericson, C.A. (2005), Hazard Analysis Techniques for System Safety, John Wiley & Sons.

[10] Nielsen, D. S. (1971), The cause-consequence diagram method as a basis for quantitative accident analysis, Risø National Laboratory, Risø-M No. 1374.

[11] Good Practice Handbook – Vol. 1 Principles & Process, iESM, 2025.

[12] Managing the Risks of Plant in the Workplace, Code of Practice, Safe Work Australia, 2018.

[13] ALCAM in Detail – An Introduction to the new ALCAM models (2014), National ALCAM Committee, 2016.