

# CORE2026

CONFERENCE ON RAILWAY EXCELLENCE

17 - 19 August 2026

Adelaide, Australia

HOSTED BY

**RTSA**

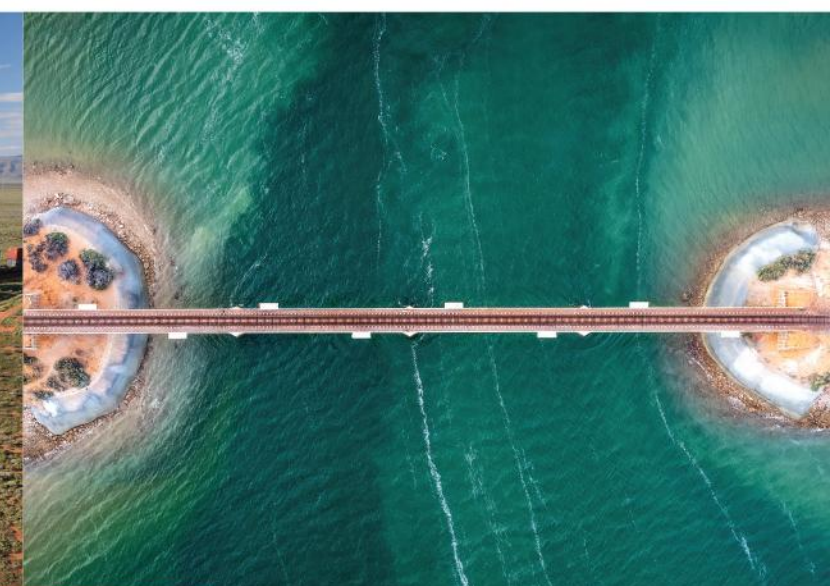
SUPPORTED BY



ENGINEERS  
AUSTRALIA



engineering  
new zealand  
te ao rangahau



[www.rtsa.com.au](http://www.rtsa.com.au)

# Effective BowTie Diagram Development

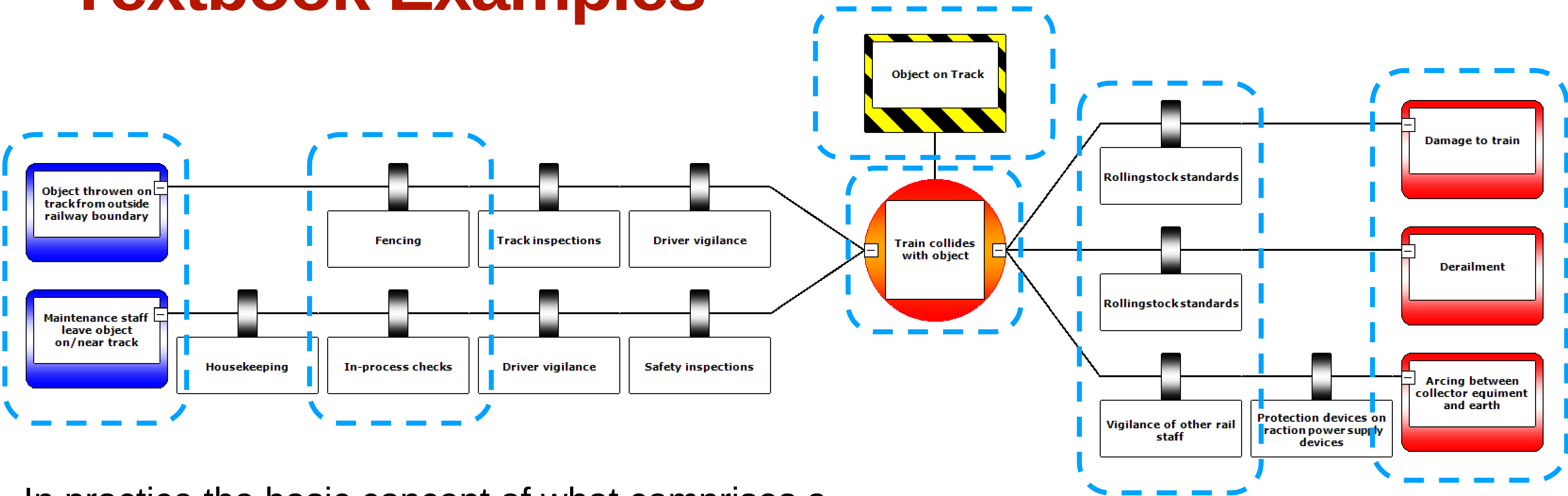
Moving Beyond Textbook Examples  
to Support Complex System Safety

Steven Gibson – ESR Consulting

# Outline

- Textbook Examples
- Selecting the Top Event
- Definitions
- Hazard 3-Tuple Framework
- Causes
- Barriers
- Cascading Scenarios
- Effective BowTies

# Textbook Examples

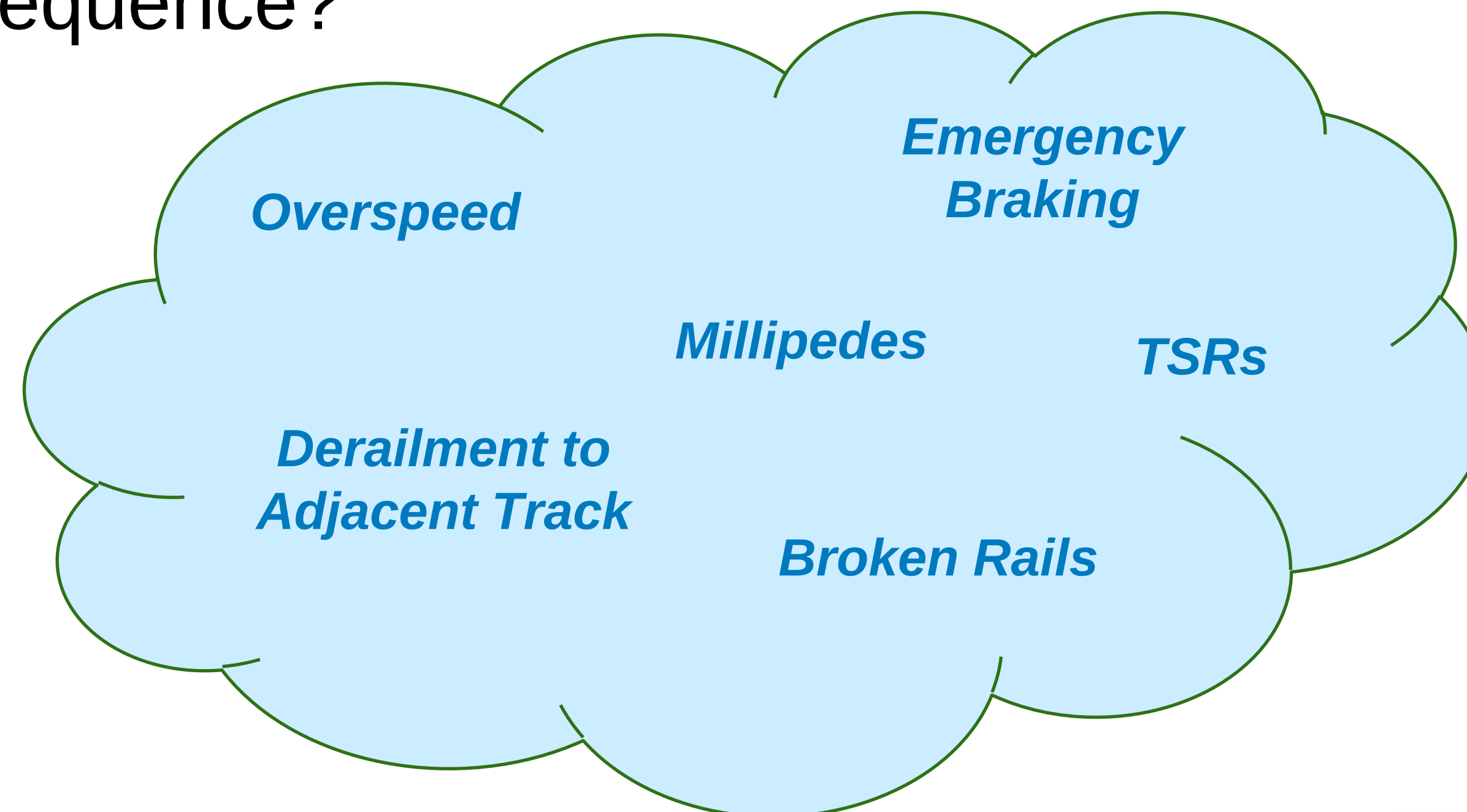


In practice the basic concept of what comprises a hazard can be difficult to define, and where poorly described can be hard to distinguish from causal factors, barriers and consequences

# Where did this paper start?

Considering **Derailment** ...

- is it a hazard?
- or an accident / consequence?
- and what about ...



# Inconsistent and Imprecise Definitions

## EN 50126-1:2017

**Hazard:** a condition that could lead to an accident.

**Accident:** an unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage.

## MIL-STD-882c

**Hazard:** a condition that is prerequisite to a mishap.

**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

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



## Other Hazard Definitions:

**IEC 61508-4:2010** – potential source of harm

**EN 50126-1:1999** - a physical situation with a potential for human injury

**EN 50129:2018** - a condition that could lead to an accident

**IEC 60050-903:2013** - potential source of harm

# The Hazard 3-Tuple Framework

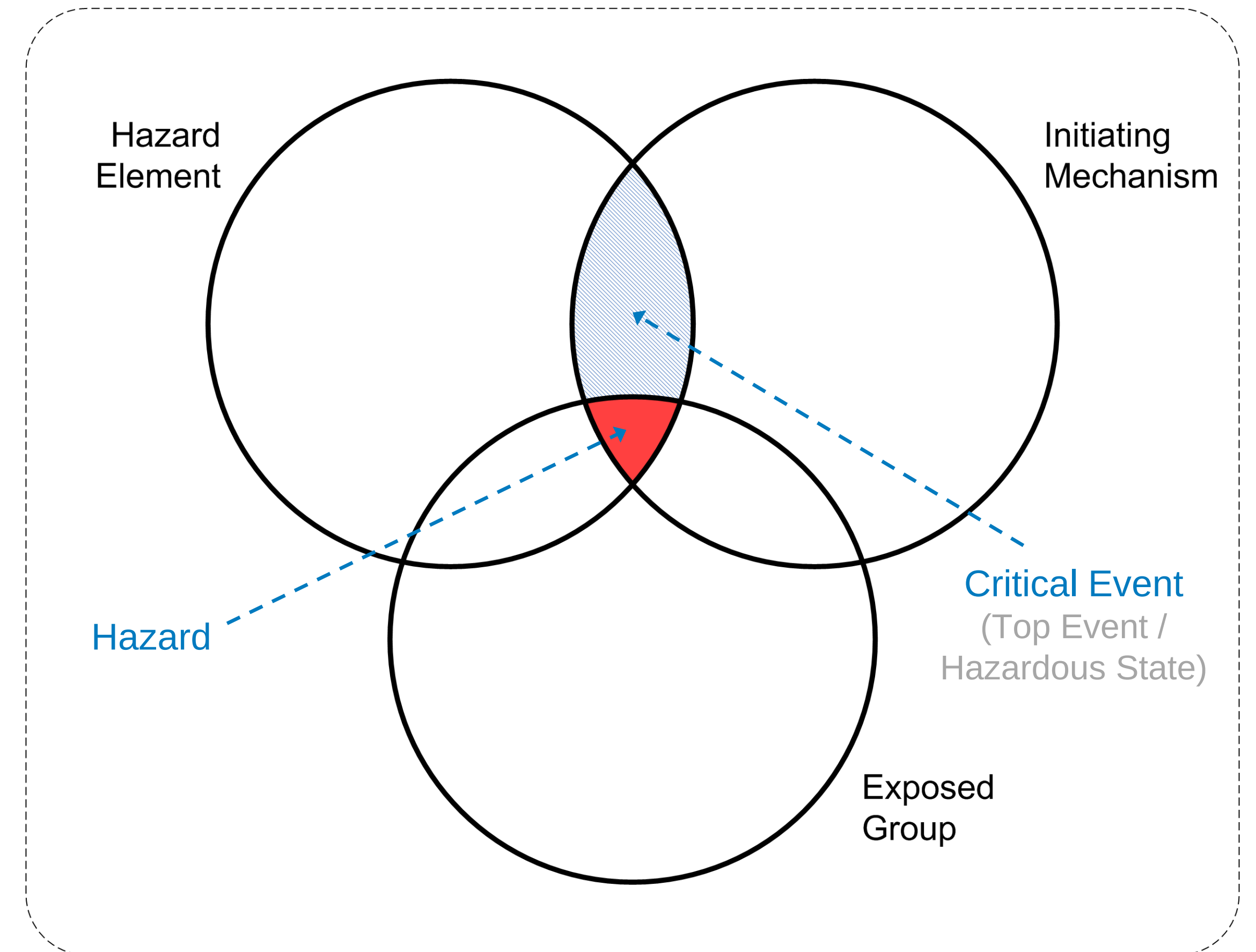
Ericson<sup>1</sup>: hazard and accident - same entity  
- state transition from *potential* event to *actual* event

Three essential interdependent components:

1. *Hazard Element (source)*
2. *Initiating Mechanism (mechanism)*
3. *Exposed Group (those with the potential for harm)*

Reduce one - *reduces the risk*

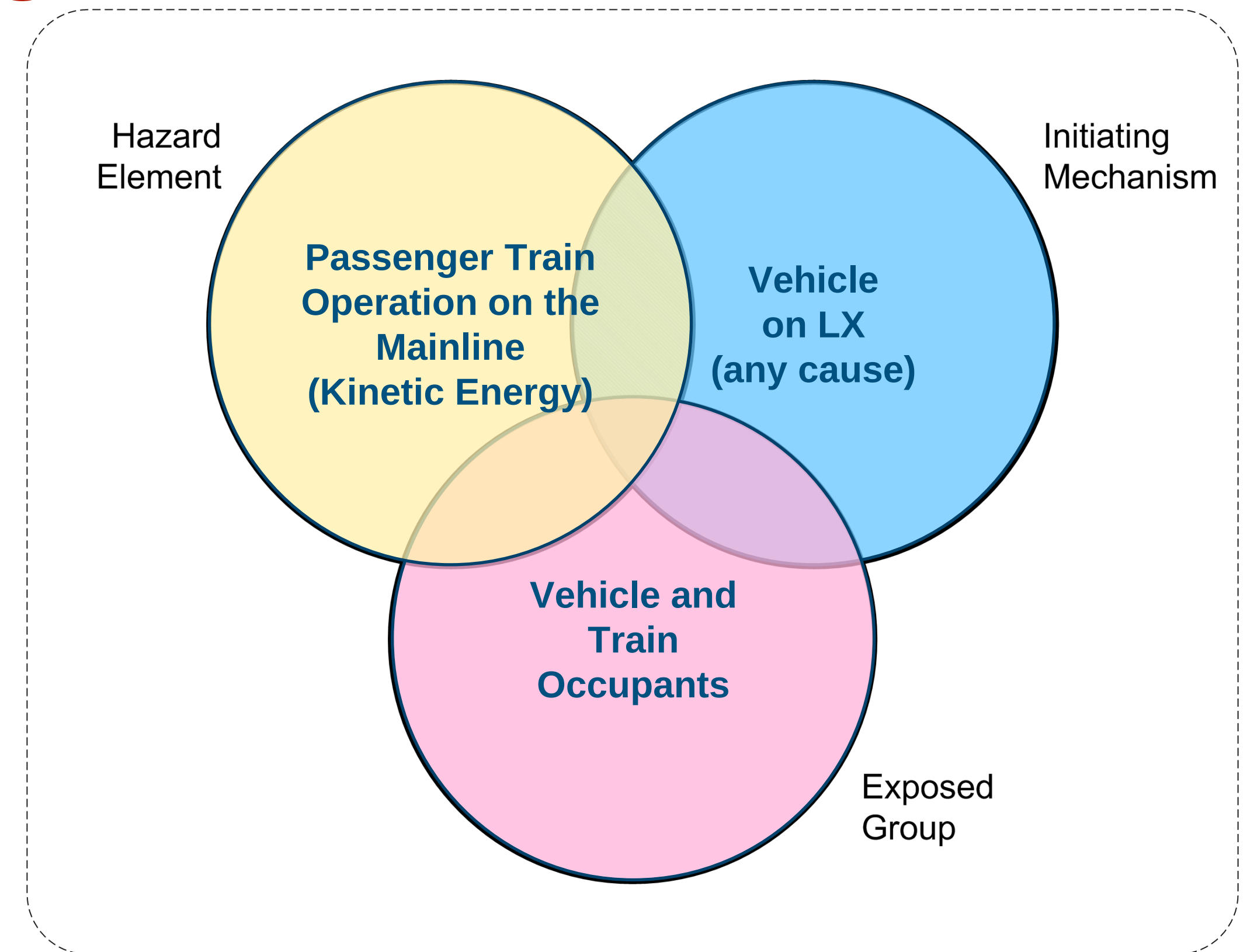
**Remove one - eliminates the hazard**



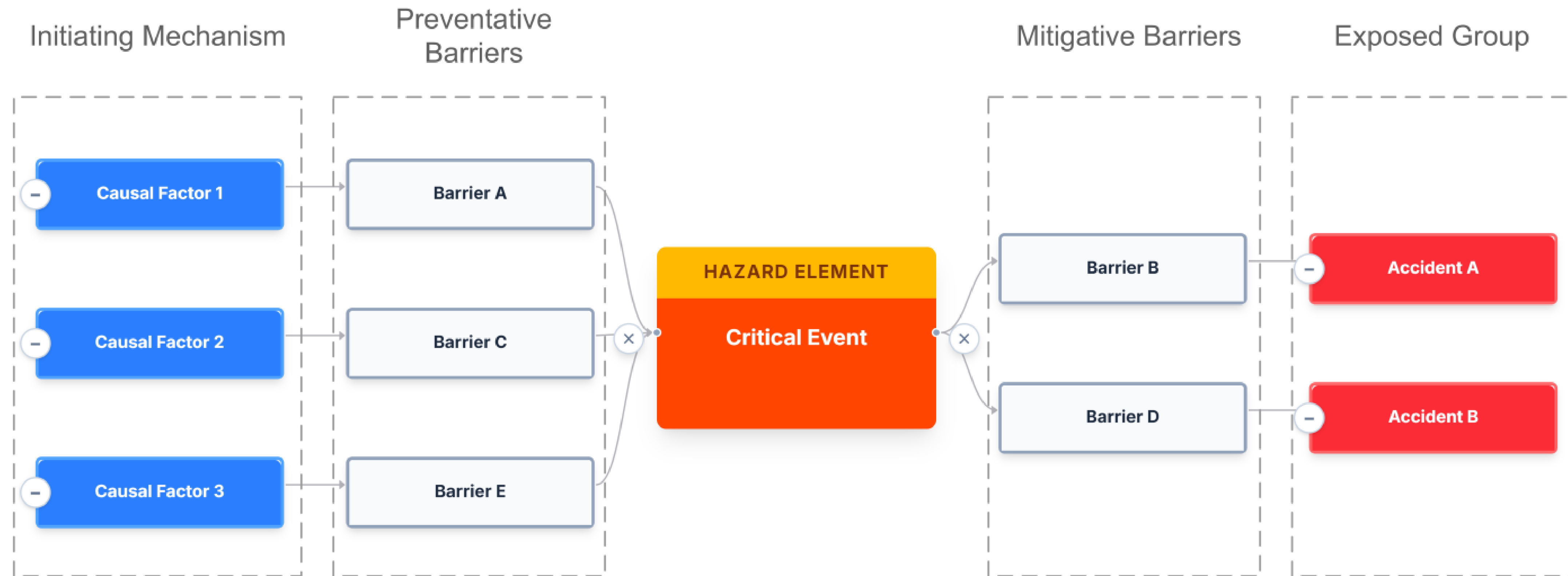
1. Ericson, C.A. (2005)  
Hazard Analysis Techniques for System Safety  
John Wiley & Sons.

# Level Crossing Example

- ✓ *Hazard Element (source)*
  - *Kinetic energy*
  - *Passenger train operation on the mainline*
- ✓ *Initiating Mechanism (mechanism)*
  - *Vehicle in the LX guideway*
  - *from any cause*
- ✓ *Exposed Group (those with the potential for harm)*
  - *Vehicle and train occupants*



# The BowTie Model



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* and to each *accident*

The *accident* description should include the *accident event*, *actor* and *harm*

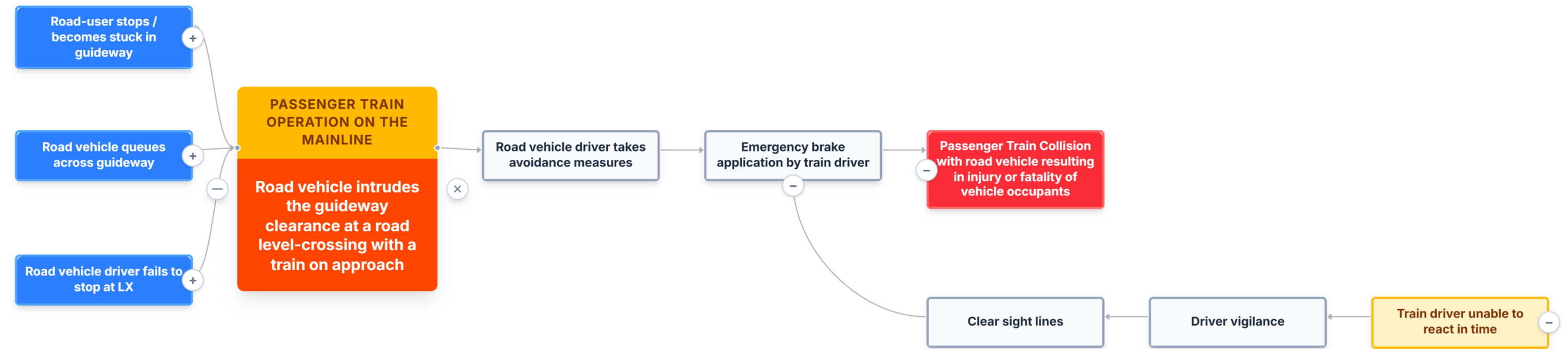
# Examples of Critical Events

| Hazard Element                                  | Initiating Mechanism                                     | Critical Event                                                         | Comment                                                                                                                                                        |
|-------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Energised high-voltage Overhead Line Equipment. | Failure to isolate OLE equipment during Maintenance.     | Arc flash during maintenance.                                          | The IM describes a failure of a control (barrier) - isolation.              |
| Energised high-voltage Overhead Line Equipment. | Maintenance activity adjacent to OLE equipment.          | Maintenance activity adjacent to OLE equipment resulting in arc flash. | The CE describes personnel exposure to a high-voltage source of energy.     |
| Driving a passenger train on the mainline.      | Lineside signal failure.                                 | Signal passed at danger.                                               | These describe failures of a control (barrier) - the signalling system.   |
| 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.   | The CE describes a loss of separation between the train and another RMV.  |

# Examples of Causal Factors

| Causal Factor                                                                 | 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.  |
| Road vehicle queues across guideway.<br>(IM is obstruction on level crossing) | 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.                            |
| Incorrect or missing TSR                                                      | Driving a passenger train on the mainline. | Overspeed leading to Passenger Train derailment.                                               | These describe failures of a control (barrier) - the TSR.                                                                                               |
| Broken Rail<br>(IM is Passenger train exceeds safe speed for track section)   | Driving a passenger train on the mainline. | Loss of control over the train's wheel-rail interface leading to Passenger Train derailment.   | The causal factor is a sufficient and credible condition to realise the critical event in combination with the hazard element.                          |

# Barriers

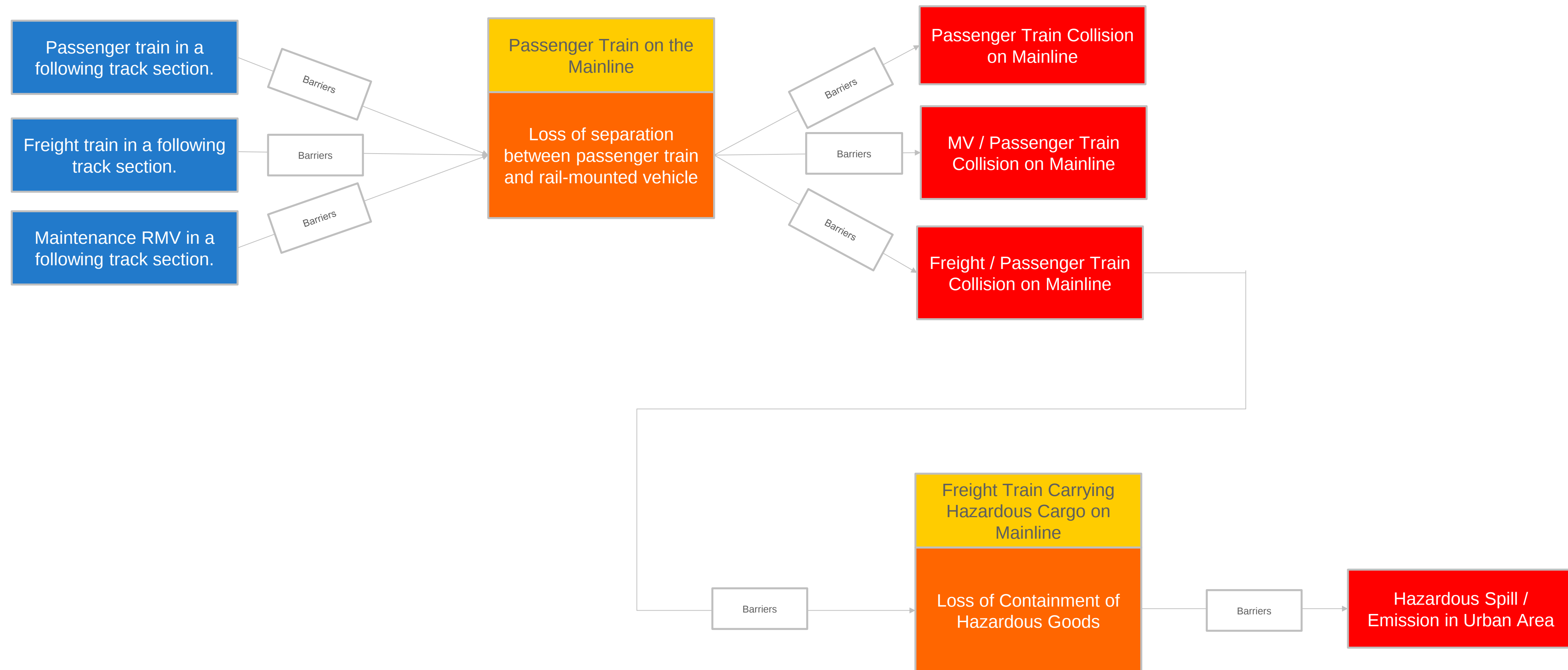


- A *preventative barrier* is one that prevents or reduces the likelihood of the *critical event* from occurring
- *Mitigative barriers* act after the *critical event* has occurred and prevents or reduces the severity of an *accident*
- Each *barrier* should be effective, independent, and not rely on other controls to function
- An *escalation factor* is a condition that can reduce the effectiveness of the preventative or mitigative *barrier* to which it is attached

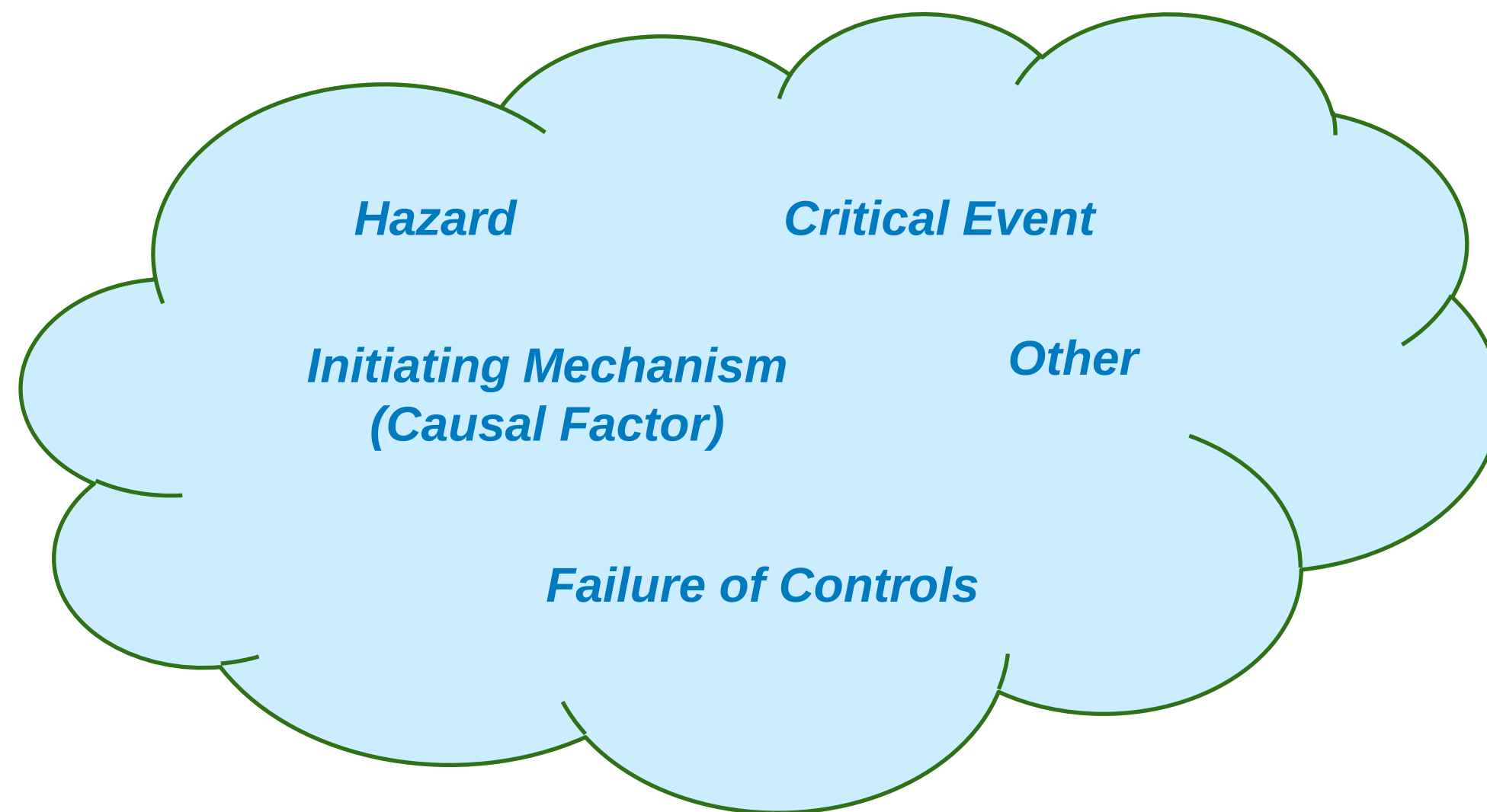
# Level Crossing Example



# Cascading Scenarios

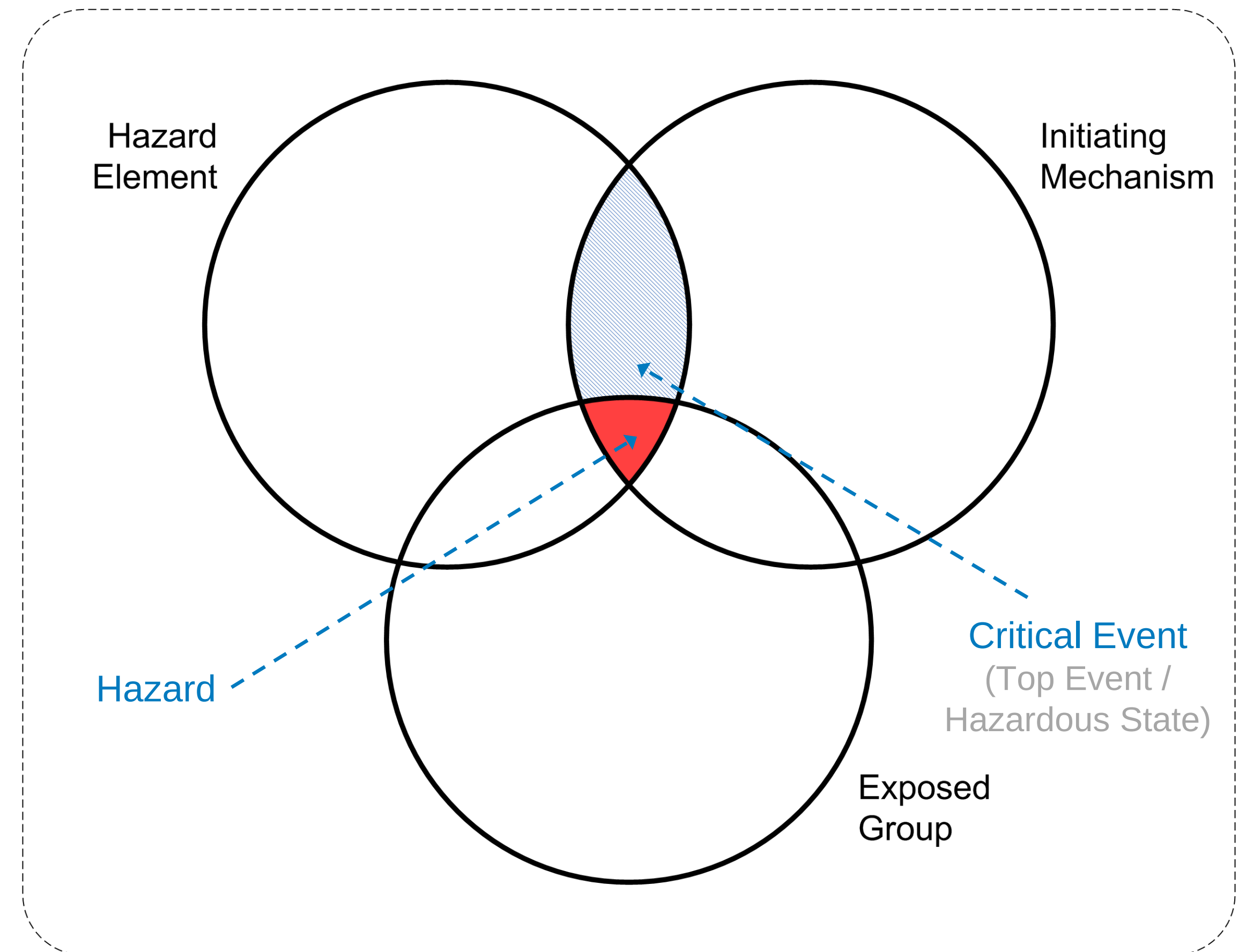


# Discuss Examples



Let's classify the following:

- Signal Failure
- Loss of train integrity / separation
- Millipedes on the track
- SPAD
- Overspeed



and thanks to ...

Kate Harding who co-authored the paper & prepared this presentation



# Questions ...

