Rail Accident Investigation Branch

Causal Analysis

The RAIB Approach
Accident investigators seminar

John Stewart

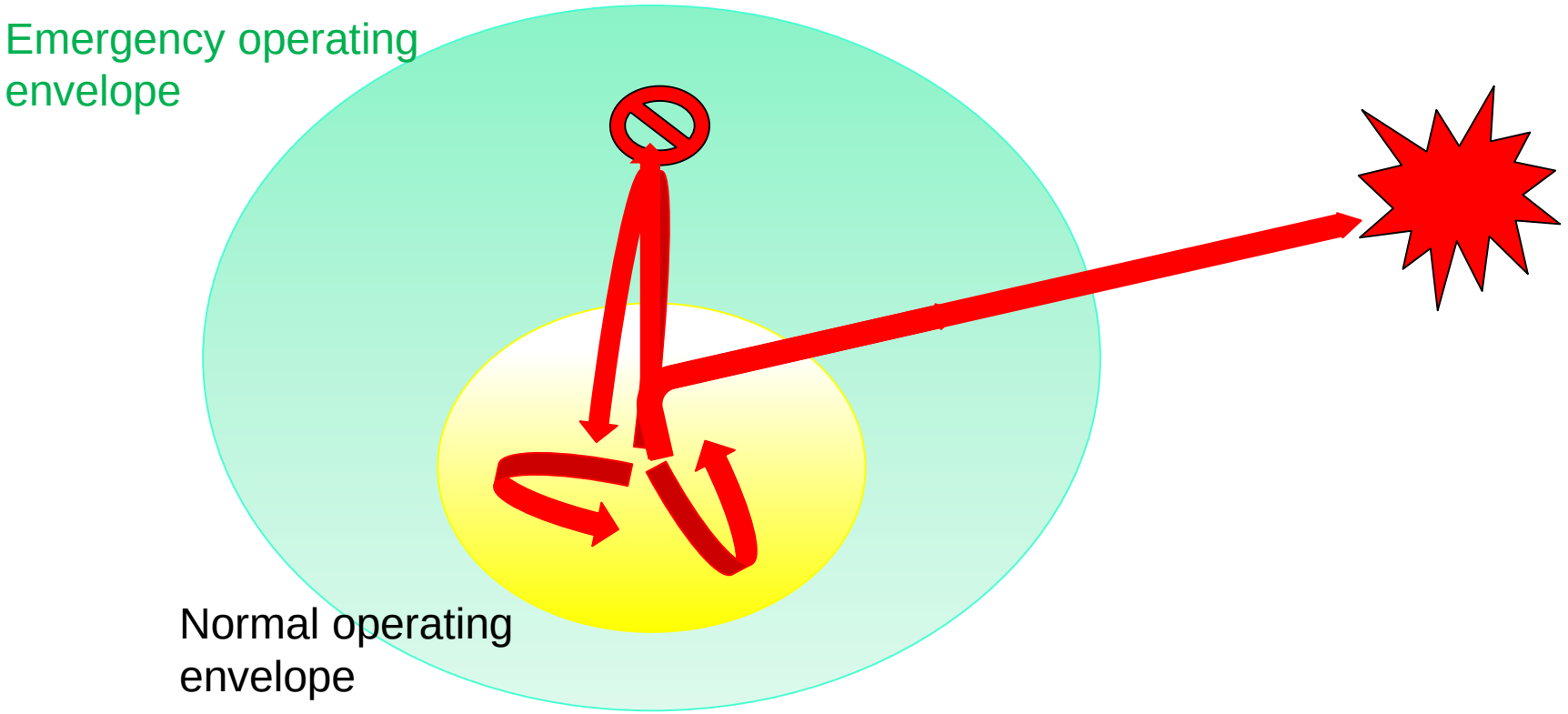
31 October 2017

Accident investigation – the job

- Collect evidence
- Analyse evidence
- Determine the cause/s of the accident
- Make recommendations to remove cause/s and/or stop them progressing to accidents
  - Improve safety

- Causal analysis assists with identifying:
    - Actions/inactions
    - Events
    - Conditions
    - Failures
  - That came together to
    - Result in the accident

Simple model



Why do accidents happen

Accident starts with

- An initial unsafe act, inaction or mech/elec/control system failure
  - System starts to deviate from the norm (normal operating envelope)

AND

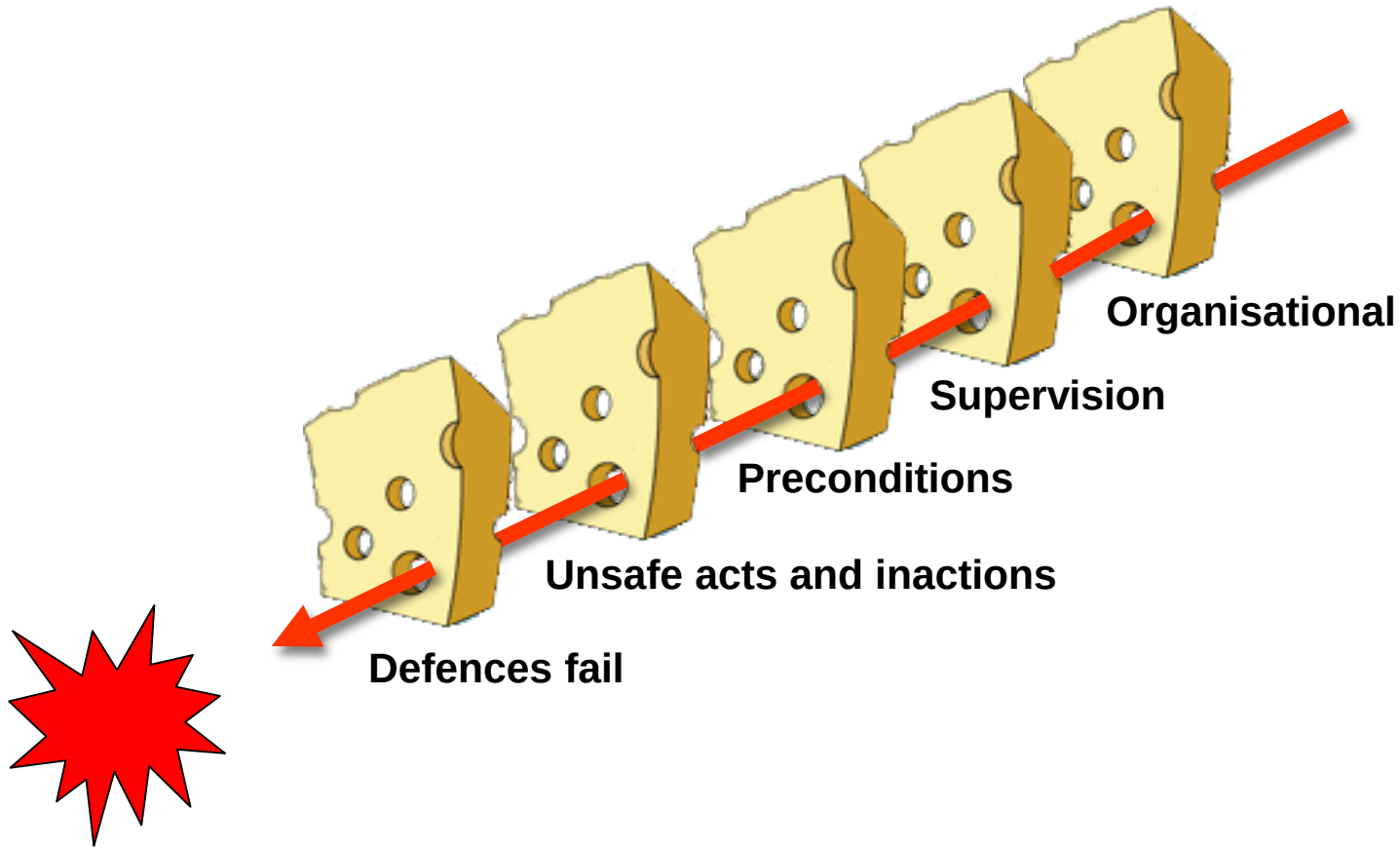
- Barrier/s designed to prevent deviation from emergency operating envelope fail to arrest the deviation

  Or

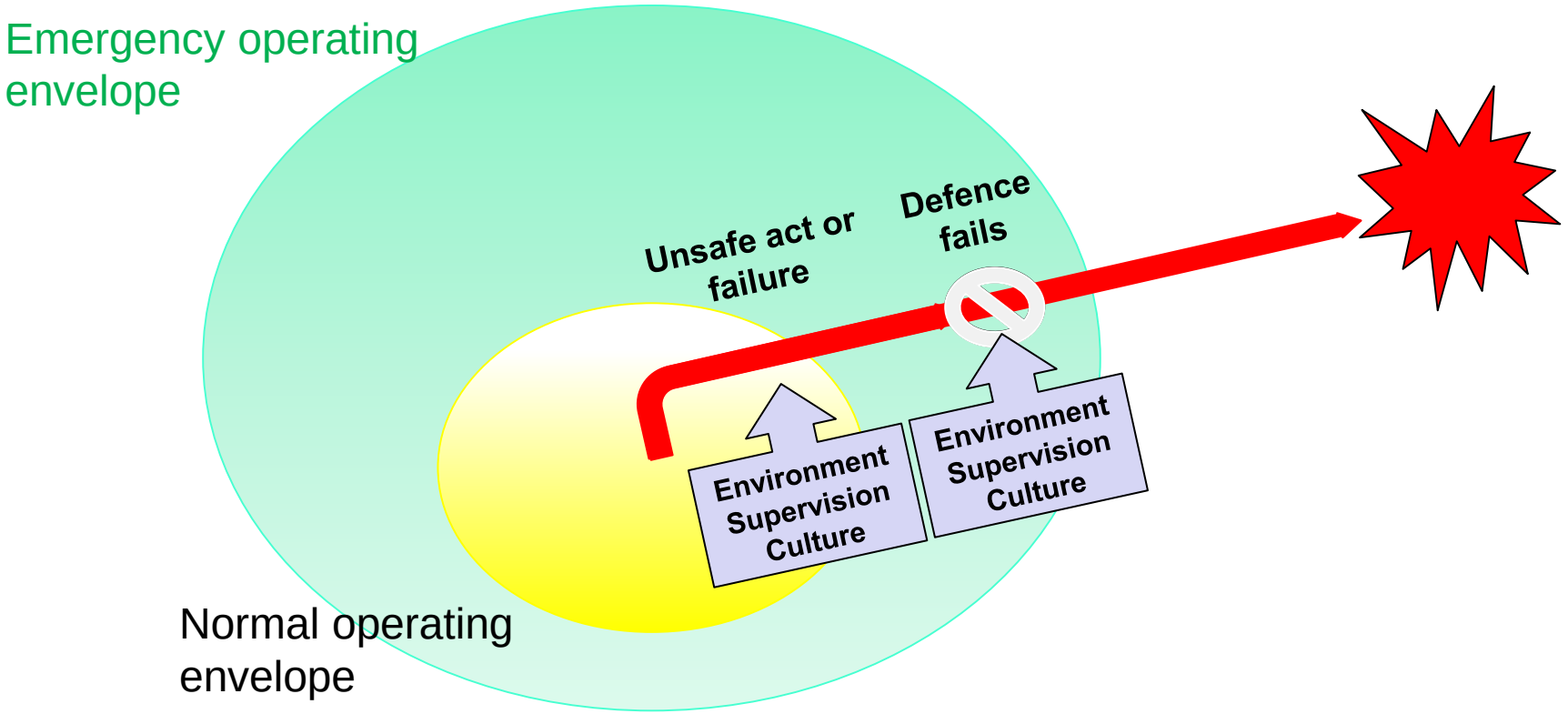
  No barrier provided
  - Barriers can be safety systems or proceduralised operator intervention

- BUT the “failures” could have been made more likely by:
  - Environment – eg interfaces, working arrangements
  - Supervision – eg training, competence, procedures
  - Culture – eg effects of (internal & external) decision makers

Reason's Accident Causation Model



Another way of thinking about it



Influencing factors (I)

- Environment
  - Factors that affect the way in which individuals and equipment perform
    - Physical – weather, ambient environment, noise, etc
    - Technological – Machine Interface, automation, checklists, etc
    - Personal – readiness, adverse physiological state, physical/mental limitations, etc
- Supervision
  - Actions taken at the supervisory, work planning, design level that set up the front line staff and/or equipment to fail.
  - Planning, specification and implementation of
    - Training, procedures and guidance, etc
    - Maintenance and inspection

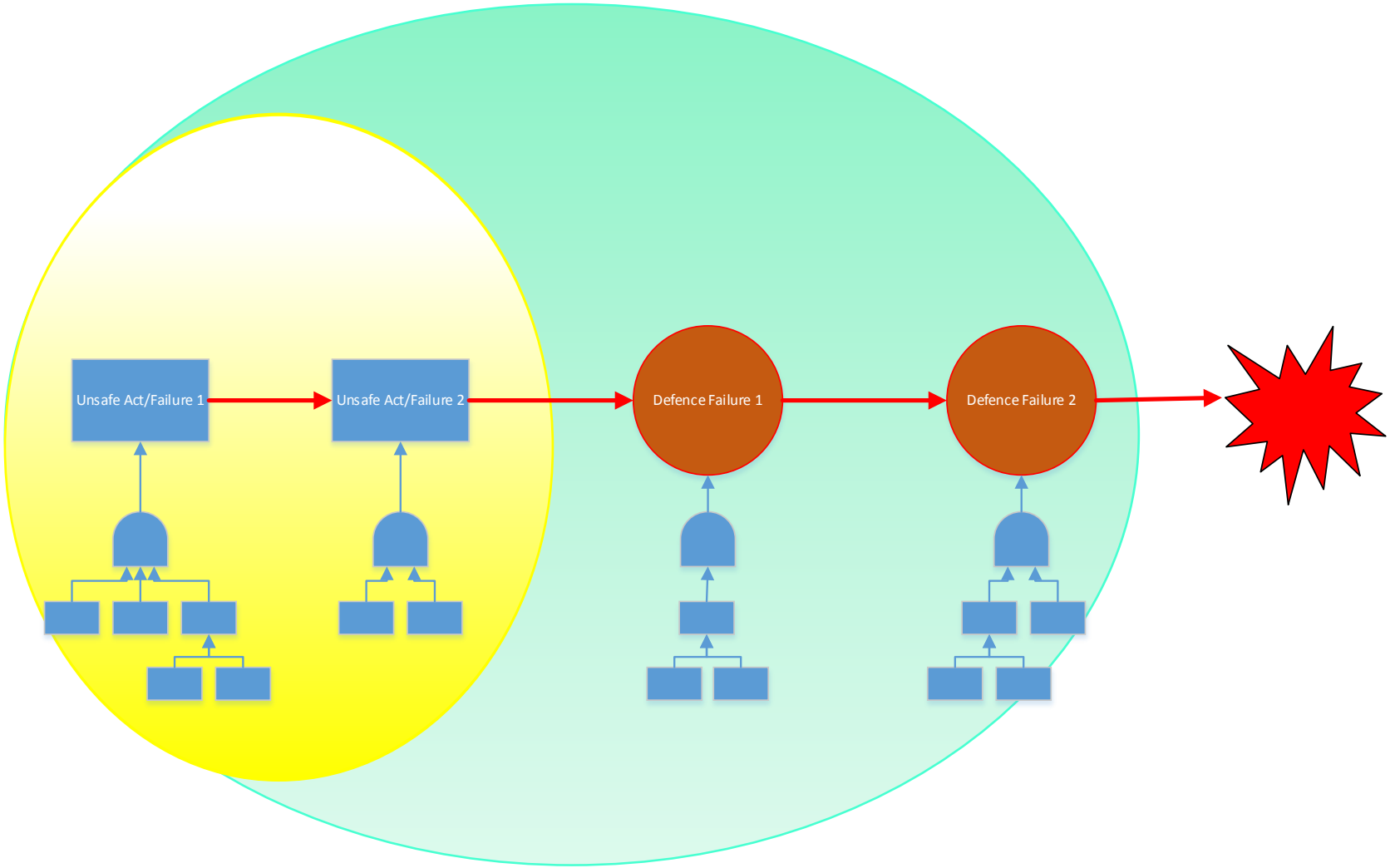
Influencing factors (II)

- ‘Culture’
  - Decisions taken at the highest level within the organisation (and possibly politically) which define
    - the whole character of the organisation
    - training policy, competence management, product safety strategy, maintenance philosophy, etc
  - Big impact on
    - what staff perceive as important,
    - degree of compliance with rules,
    - attitude to learning, etc
  - Interested in what elements of it had an impact on unsafe acts and failures

Example influencing factors

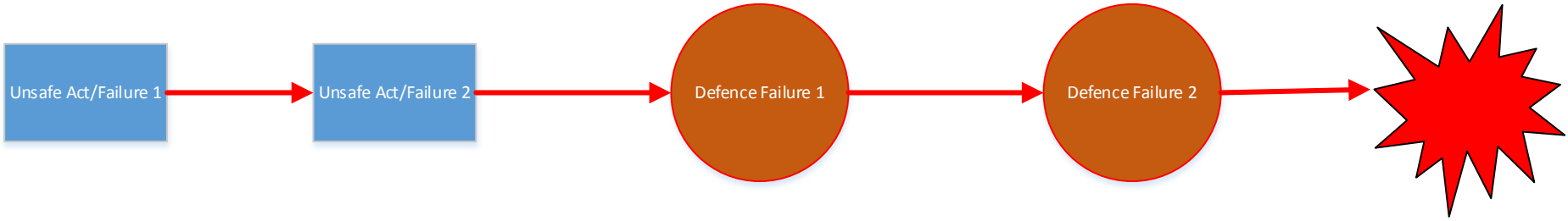
- Human errors:
  - Rules, procedures and instructions
  - Training and knowledge
  - Personal capability
  - Communications
  - Work place engineering & ergonomics
  - Workload
  - Line Supervision and selection
  - Quality assurance and control
  - Management systems
  - Contractual responsibilities
- System & equipment failures:
  - Incomplete or incorrect design specification
  - Design not complying with the specification
  - Not suitable for actual environment
  - Inadequate or incorrect checking, inspection, maintenance or calibration
  - Undetectable or unannounced faults and failures
  - Low fault tolerance of the design
  - Impact of changes not fully assessed
  - Inadequate risk assessment

Structure of the RAIB approach



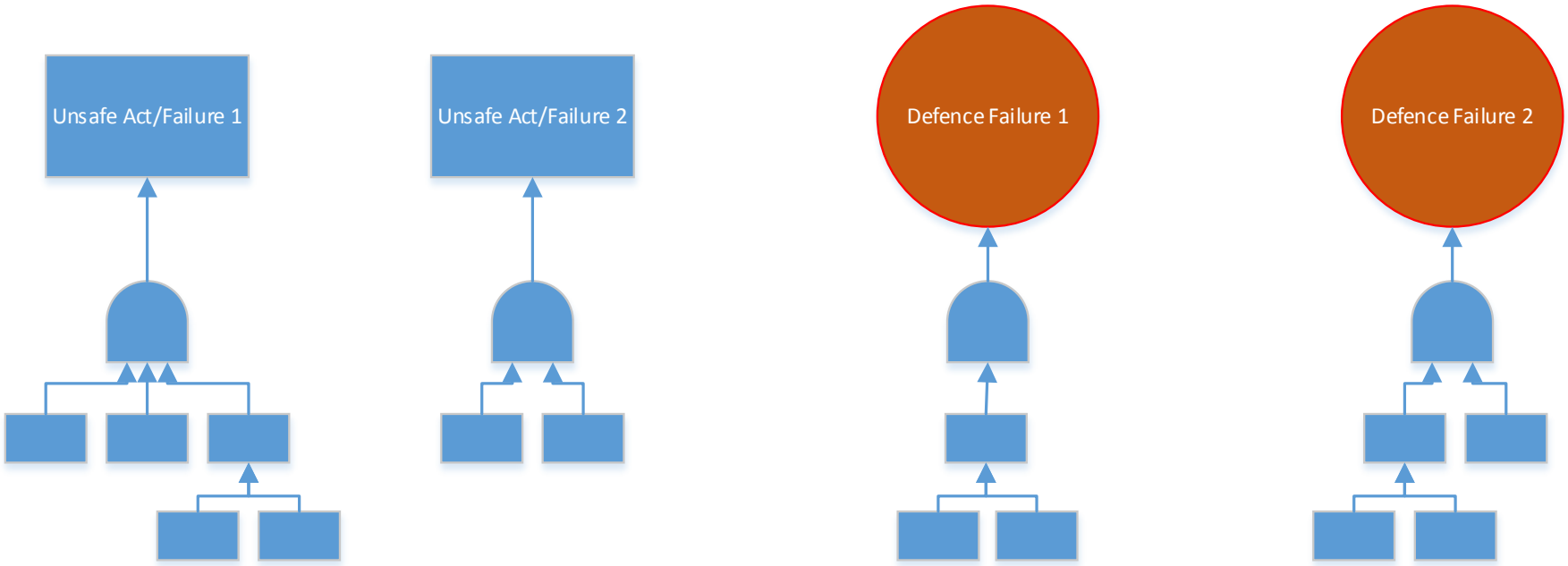
RAIB process – 2 elements (1)

Sequence of events

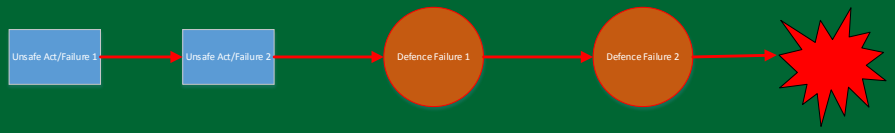


RAIB process – 2 elements (2)

Failure analyses

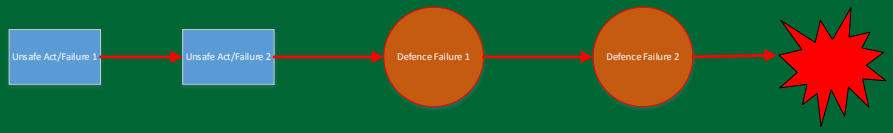


Sequence of Events



- Sequence Time Event Plot (STEP)
- Each actor (or party) involved in the accident identified in a swim lane, eg
  - equipment, infrastructure & technical systems
  - people
  - organisations
  - etc
- Plot events relevant to each actor horizontally in a sequential manner
- Add causal linkages
- Identify where barriers should have prevented progression
- Link evidence confirming events
- Events on the sequence diagram will be:
  - Normal events
  - Extreme events
  - Fault events

Sequence of Events Example



Fire in Tunnel – example only

Loading and departure

Lorry

- Date: 17/01/2015 Time: ? Conf.Level: 100% 0 — Lorry enters depot
- Date: 17/01/2015 Time: ? Conf.Level: 100% 0 — Lorry allocated to wagon A
- Date: 17/01/2015 Time: 11:46:12 Conf.Level: 100% 0 — Lorry passes detection system.
- Date: 17/01/2015 Time: 11:46:40 Conf.Level: 100% 0 — Lorry boards the train.
- Date: 17/01/2015 Time: 11:47:25 Conf.Level: 100% 0 — Lorry stops on penultimate wagon.
- Date: 17/01/2015 Time: 12:00:08 Conf.Level: 100% 0 — Arcing event between the lorry and the overhead power line.

Allocation team

- Date: 17/01/2015 Time: ? Conf.Level: 100% 0 — No defect identified by agents (x2) and CCTV operator during allocation

Train

- Date: 17/01/2015 Time: ? Conf.Level: 100% 0 — Train arrives at platform 3.
- Date: 17/01/2015 Time: ? Conf.Level: 100% 0 — Unloading of train starts.
- Date: 17/01/2015 Time: 11:42:30 Conf.Level: 100% 0 — Loading of train starts.
- Date: 17/01/2015 Time: 11:55:00 Conf.Level: 100% 0 — All passengers on-board.
- Date: 17/01/2015 Time: 11:57:00 Conf.Level: 100% 0 — Train departs platform 3.
- Date: 17/01/2015 Time: 11:59:40 Conf.Level: 100% 0 — Leading loco enters the tunnel.
- Date: 17/01/2015 Time: 12:01:38 Conf.Level: 100% 0 — Train comes to a stop in tunnel.
- Date: 17/01/2015 Time: 12:03:36 Conf.Level: 100% 0 — Train restarts its journey.

Unloading / loading team

- Date: 17/01/2015 Time: 11:46:30 Conf.Level: 50% 0 — Lorry inspected.
- Date: 17/01/2015 Time: 11:48:00 Conf.Level: 50% 0 — Lorry chocked.

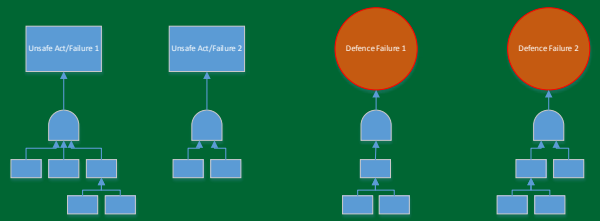
Loaders

- Date: 17/01/2015 Time: ? Conf.Level: 100% 0 — Loaders start to leave platform.
- Date: 17/01/2015 Time: ? Conf.Level: 100% 0 — Loaders watch train as it leaves.
- Date: 17/01/2015 Time: ? Conf.Level: 100% 0 — Loader sees obstruction briefly but takes no action.

Control

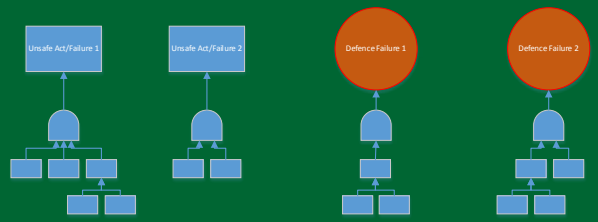
- Date: 17/01/2015 Time: ? Conf.Level: 100% 0 — Control allows train to continue in service

Failure Analysis



- Fault tree based why because analysis
  - Allow for weak causal links – influencing factors
- For each fault event - written in terms of the failure that occurred
  - Identify the [immediate] precursor conditions/events that led to the fault event (singularly or in combination).
  - These can normally be determined by asking “Why” or “What led to ...”
    - Where not
      - Supplement with other specific causal analysis techniques
      - Undertake additional testing/analysis
- Repeat to next level in a step wise manner
  - Until reach bottom event which cannot usefully be broken down any further
- Identify where barriers should have prevented progression up the tree
- Identify whether any factors could have influenced bottom events
  - Environmental, supervision and culture issues
- Link evidence confirming events and their consequences to each event

Failure Analysis – Example I



Fire on train in tunnel

Date: 17/01/2015 Time: Conf.Level: 100% 0
A lorry with out of gauge load.

Date: 17/01/2015 Time: Conf.Level: 100% 0
Train with out of gauge load allowed to depart

Date: 17/01/2015 Time: Conf.Level: 100% 0
The initial arcing event al did not lead to the identification of the start of a fire.

Date: 17/01/2015 Time: Conf.Level: 100% 0
Out of gauge detection system failed

Date: 17/01/2015 Time: Conf.Level: 100% 0
Protective barriers removed

E 11 InterviewXYZ

Date: 17/01/2015 Time: Conf.Level: 100% 0
Manual observation not followed through.

Date: 17/01/2015 Time: Conf.Level: 100% 0
No examination of train to confirm the origin of the power trip

Date: 17/01/2015 Time: Conf.Level: 100% 0
Procedures allow for reset and go in terms of power trip.

E 15 ABC meeting

E 13 Lorry height analysis

E 18 AAA testing

100%
Out of gauge detection system cannot reliably detect small exceedances.

E 19 DEF info

100%
Original wagon design was poor

100%
Inadequate safety justification

25%
Train design not modified

E 15 ABC meeting

E 15 ABC meeting

E 11 InterviewXYZ

100%
Operative was unsure load was out of gauge

100%
There was no supervisor available to provide guidance

E 11 InterviewXYZ

100%
Lack of reference point (OLE higher at platform than in tunnel).

E 11 InterviewXYZ

100%
OLE power trip not associated with the possible start of a fire.

100%
Power trips are not unusual on an electrified railway.

E 16 Analysis of catenary trip

100%
Fire incident only declared after 12 minutes.

E 21 Review of submission

100%
Supplier arguments not ALARP

100%
Regulator accepted justification

E 22 Reg meeting

E 23 ISA authorisation

100%
Inexperienced operative.

E 11 InterviewXYZ

100%
Speed of passage in front of sensors.

100%
Sesnsitivity of sensors

E 20 Speed of passage assessment

E 19 DEF info

E 21 Review of submission

100%
Control measures not related to personal safety

100%
ISA review did not identify spurious arguments

100%
Adequacy of procedures?

E 17 Prbcedure review

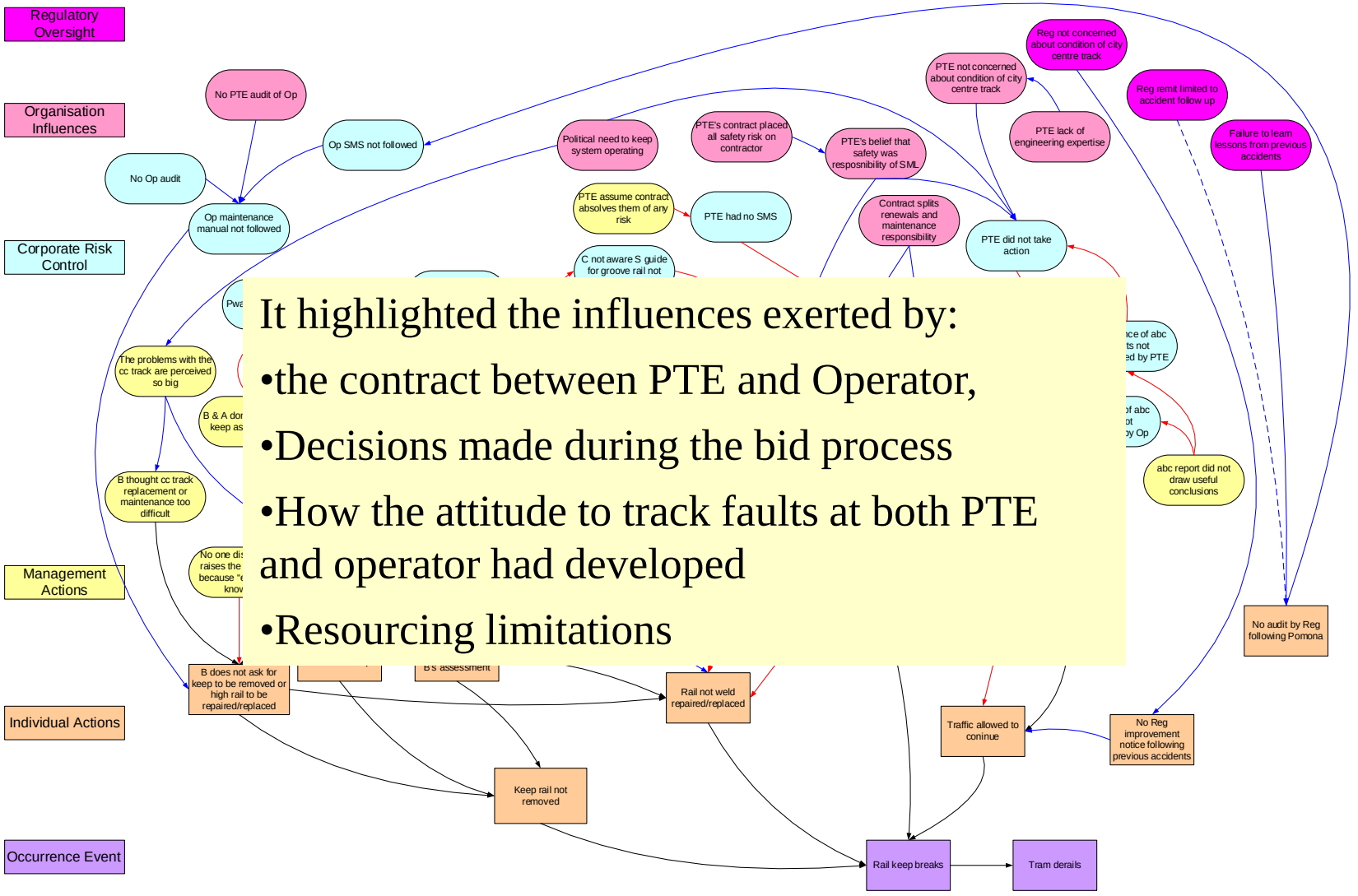
Failure Analysis - Supporting tools/techniques

- FMEA – failure modes and effects analysis
  - When we cannot understand what led to a factor
  - Understand all failure modes – “bottom up”
  - Each potential failure mode for a system is identified and analysed to determine its effect on the top level system.
    - Break the system down into its parts or functions
    - Identify the failure modes that cause the part to lose functionality
    - Determine consequence of failure mode at system level
  - The evidence can then be reviewed or additional testing undertaken to understand which failure modes are credible

Failure Analysis - Supporting tools/techniques

- AcciMap
  - Means to understanding relationships in complex sociotechnical systems
  - When need to better understand influences on behaviour, particularly at an organisational or regulatory level
  - Structure to analyse the relationship between actions and events at a variety levels:
    - local,
    - industry,
    - regulatory
    - political

Accimap – Tramway derailment



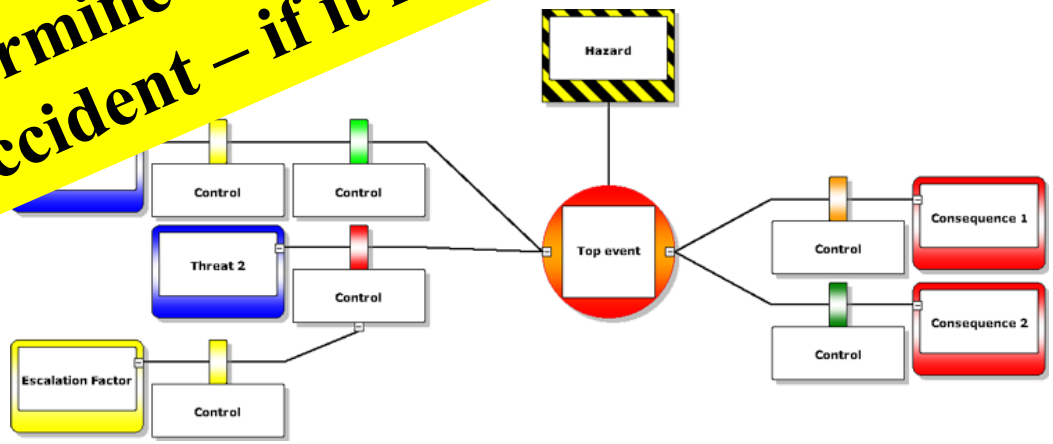
It highlighted the influences exerted by:

- the contract between PTE and Operator,
- Decisions made during the bid process
- How the attitude to track faults at both PTE and operator had developed
- Resourcing limitations

Bow Tie Analysis

- Design based tool
- Starts with hazard
  - Identifies possible caus
  - consequences o
- Causes tak
- Co
- consequences
c

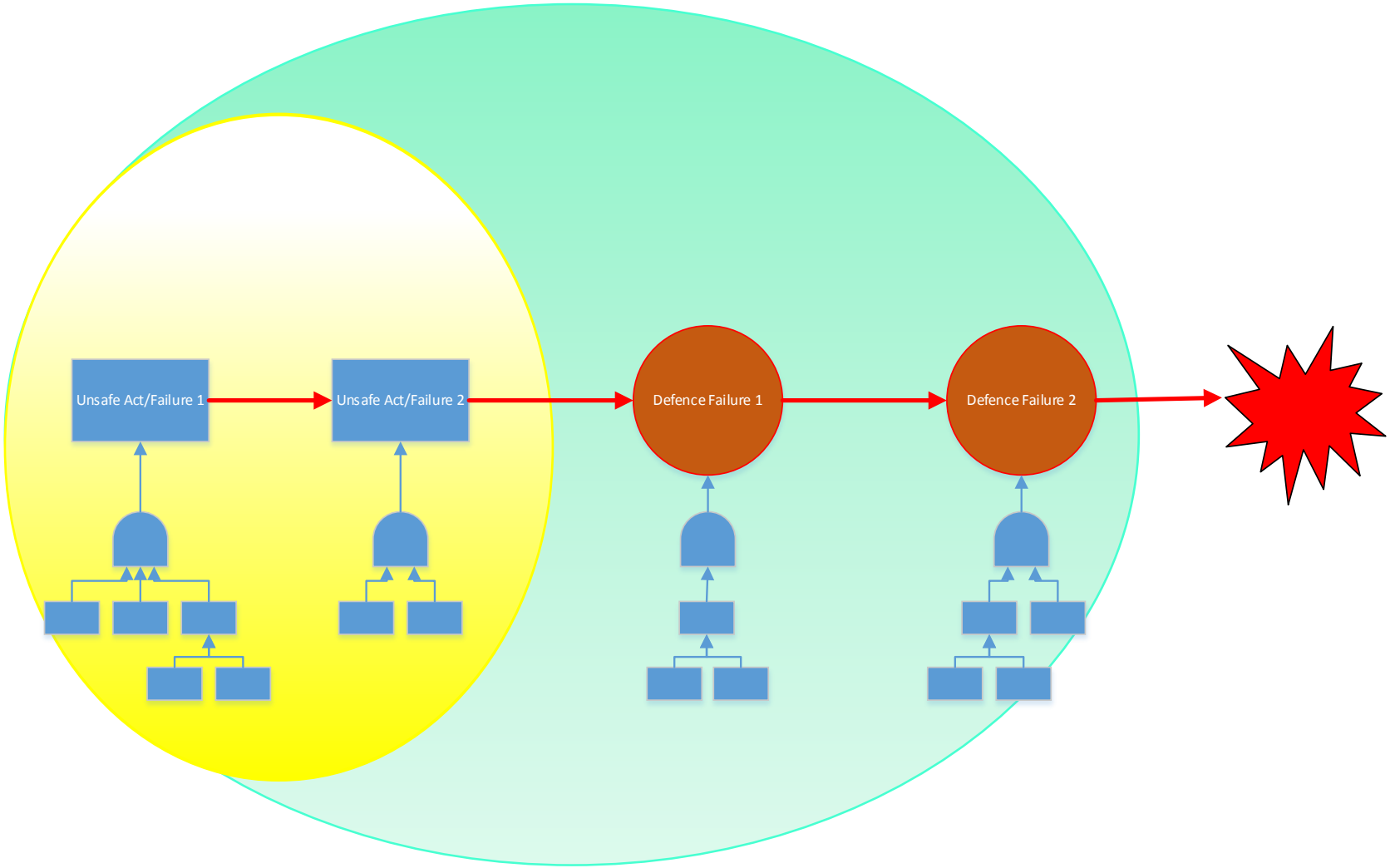
As accident investigators
If we are lucky enough there will be a bow tie diagram for our hazard
We will be able to review it against the available evidence to determine the one path through it that led to our accident – if it has been modelled!



Two final points

- Evidence
  - Link evidence to Sequence of Events and Failure Analysis
    - Proves that action, etc occurred
    - Proves causal/consequential linkage
  - Identifies additional investigation, analysis and/or testing
- Recommendations
  - Review the failures
    - Identify whether a recommendation is appropriate to prevent reoccurrence
  - Review the following to identify whether additional safety barriers would have been appropriate
    - Sequence of events
    - Failure Analysis

Recommendations – remove the events and break the links



Process Summary

- Sequence of events diagram
  - Key purpose is to identify relevant fault events
- Failure Analysis
  - Key purpose is to understand factors causing each fault event
  - Both direct factors and influencing factors
- Evidence mapping
  - Key purpose is to demonstrate confidence with findings
- Recommendations driven from
  - Sequence of events
  - Failure analysis