ENGINEERS AUSTRALIA

ASEW

AUSTRALIAN SYSTEMS ENGINEERING WORKSHOP

ADELAIDE | 1-2 NOVEMBER 2018

ENGINEERS AUSTRALIA SESA

INCOSE

Katherine Eastaughffe

Can Better Systems Engineering Practice Lead To More Efficient Assurance Of Rail Projects?

What is Assurance?

Reference	Term	Definition Provided
UK Rail Safety and Standards Board (RSSB) [1]	Assurance	A positive declaration intended to give confidence
	Supplier Assurance	The generic term for actions, processes and procedures applied by a customer, to ensure effective use of suppliers
	Safety Assurance	Confidence that risks, behaviours and processes that are potential threats to safety are being managed and controlled to acceptable levels through appropriate measures
UK National Audit Office [5]	Assurance	An independent assessment of whether the required elements to deliver projects successfully, such as good project management practices and appropriate funding and skills, are in place and operating effectively
Association of Project Managers [10]	Project Assurance	The process of providing confidence to stakeholders that projects, programmes and portfolios will achieve their scope, time, cost and quality objectives, and realise their benefits
HB 158—2010 Delivering assurance based on ISO 31000:2009 Risk Management — Principles and guidelines	Assurance	A process that provides a level of confidence that objectives will be achieved within an acceptable level of risk
Transport for London (TfL) Integrated Assurance Framework [7]	Assurance	The means by which a party responsible for a business activity and its stakeholders gain confidence in the appropriateness of the organisation’s decision making and the effectiveness of internal controls

Reference	Term	Definition Provided
Transport for New South Wales (TfNSW) Assets Standards Authority (ASA)	Assurance	An objective examination of evidence for the purpose of providing an independent assessment of risk management, management control or governance processes for an organisation. [8]
		Assurance is a set of structured and planned activities conducted through the asset life cycle providing progressive justified confidence that objectives are being achieved and that the asset is or will be fit for purpose. [10]
		A positive declaration intended to give confidence [9]
	Engineering Assurance	The evidence that planned outcomes have been achieved, or the evidence of effective management of risk [9]
	Systems Assurance	Systems assurance is the planned and systematic set of activities that demonstrate how the systems and products shall conform to requirements for safety, reliability, availability, maintainability, standards, procedures, and regulations. [9]
	Safety Assurance	Demonstration that all safety risks have been assessed and managed/mitigated SFAIRP (So Far As Is Reasonably Practicable) and satisfy the risk tolerability criteria. [8]
US APTA (American Public Transportation Association) Rail Conference Paper [8]	Systems Assurance	Systems assurance management is a framework for transit agencies and their contractors to ensure systems have been designed, constructed, and operated considering all critical factors related to safety, reliability, availability, and maintainability
North Atlantic Treaty Organisation (NATO) [9]	System Assurance	Justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle
US Air Force Space Command Design Assurance Guide [10]	Design Assurance	Design assurance is a formal, systematic process that augments the design effort and increases the probability of product design conformance to requirements and mission needs. The activity associated with design assurance has, as its objective, a truly independent assessment of the overall process for development of engineering drawings/models/analyses and specifications

An independent assessment of whether the required elements to deliver projects successfully, are in place and operating effectively.

A process that provides a level of confidence that objectives will be achieved within an acceptable level of risk.

Systems assurance is the planned and systematic set of activities that demonstrate how the systems and products shall conform to requirements for safety, reliability, availability, maintainability, standards, procedures, and regulations.

A positive declaration intended to give confidence

The means by which a party responsible for a business activity and its stakeholders gain confidence in the appropriateness of the organisation's decision making and the effectiveness of internal controls

Design assurance is a formal, systematic process that augments the design effort and increases the probability of product design conformance to requirements and mission needs.

Assurance is a set of structured and planned activities conducted through the asset life cycle providing progressive justified confidence that objectives are being achieved and that the asset is or will be fit for purpose.

ASSURANCE/ SYSTEM ASSURANCE?

- Safety (Rail, WHS, System, Functional)
- RAM (Reliability, Availability, Maintainability)
- Human Factors
- Security (Cybersecurity)
- EMC
- Standards Compliance
- Requirements Compliance
- Quality

What is Assurance?

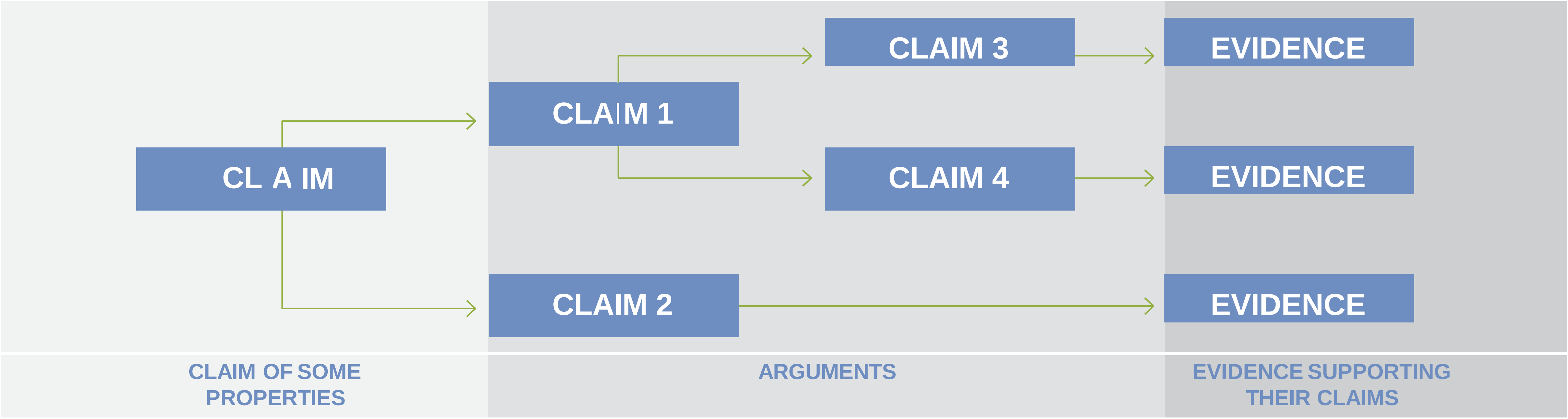
- What should the definition of assurance be?
- Is it just concerned with safety?
- How is it different to V&V
- If not, what else is it concerned with?

Best Definition of Assurance

- ISO/IEC 15026-1:2013 Systems and Software Engineering – Systems and Software Assurance

> *Grounds for justified confidence that a claim has been or will be achieved*

Assurance Cases



CL A IM

CLAIM 1

CLAIM 2

CLAIM 3

CLAIM 4

EVIDENCE

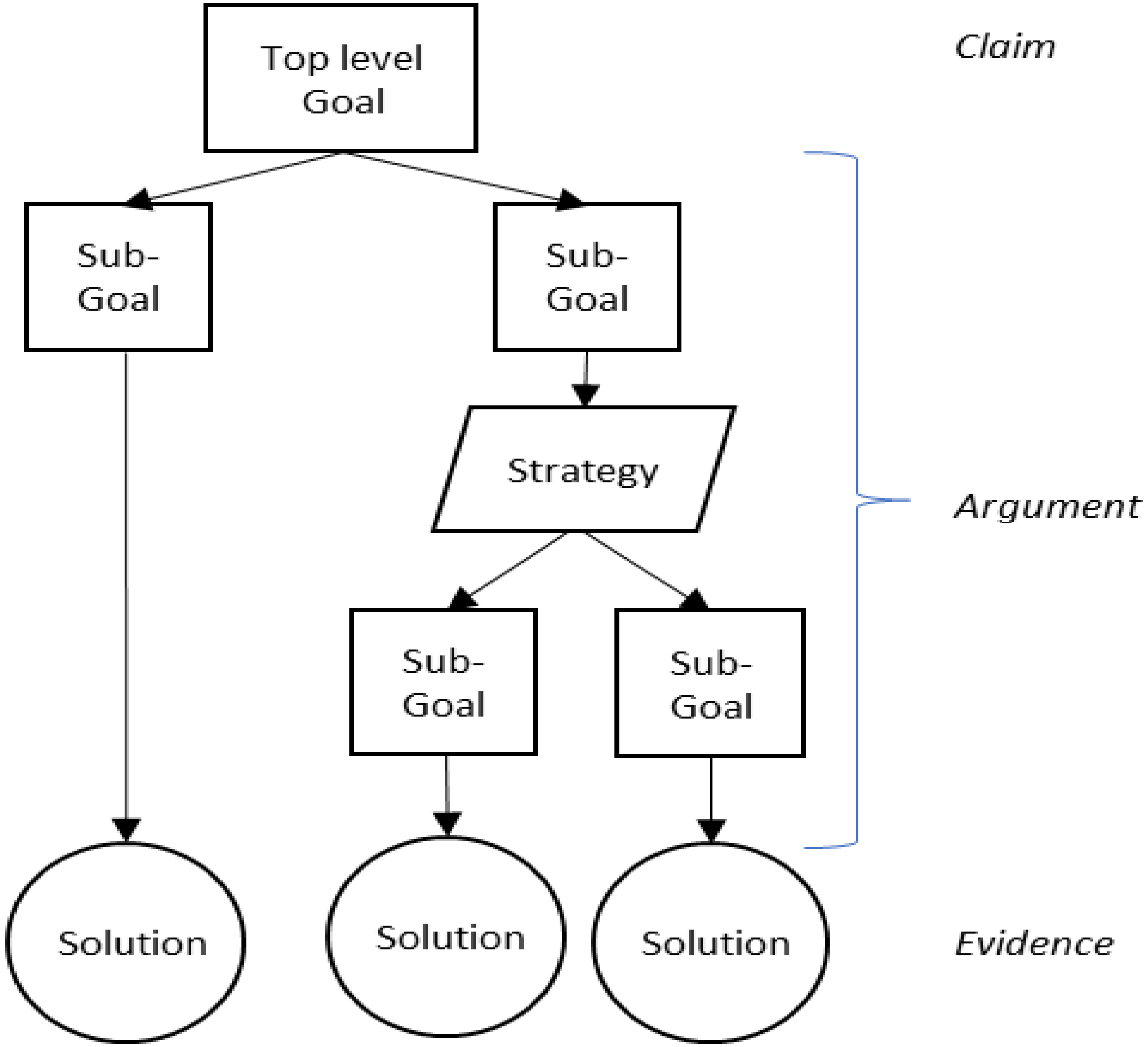
EVIDENCE

EVIDENCE

CLAIM OF SOME PROPERTIES

ARGUMENTS

EVIDENCE SUPPORTING THEIR CLAIMS



Top level Goal

Sub-Goal

Sub-Goal

Strategy

Sub-Goal

Sub-Goal

Solution

Solution

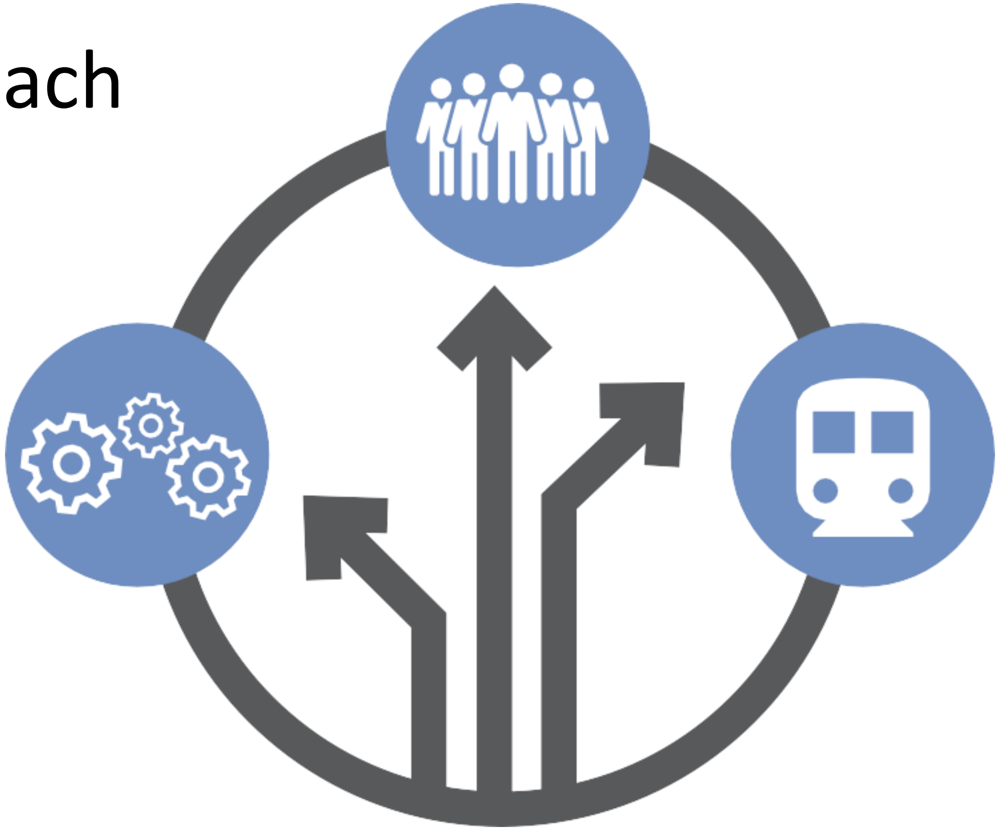
Solution

Claim

Argument

Evidence

Emergent Performance



Reach

Safety

Ease

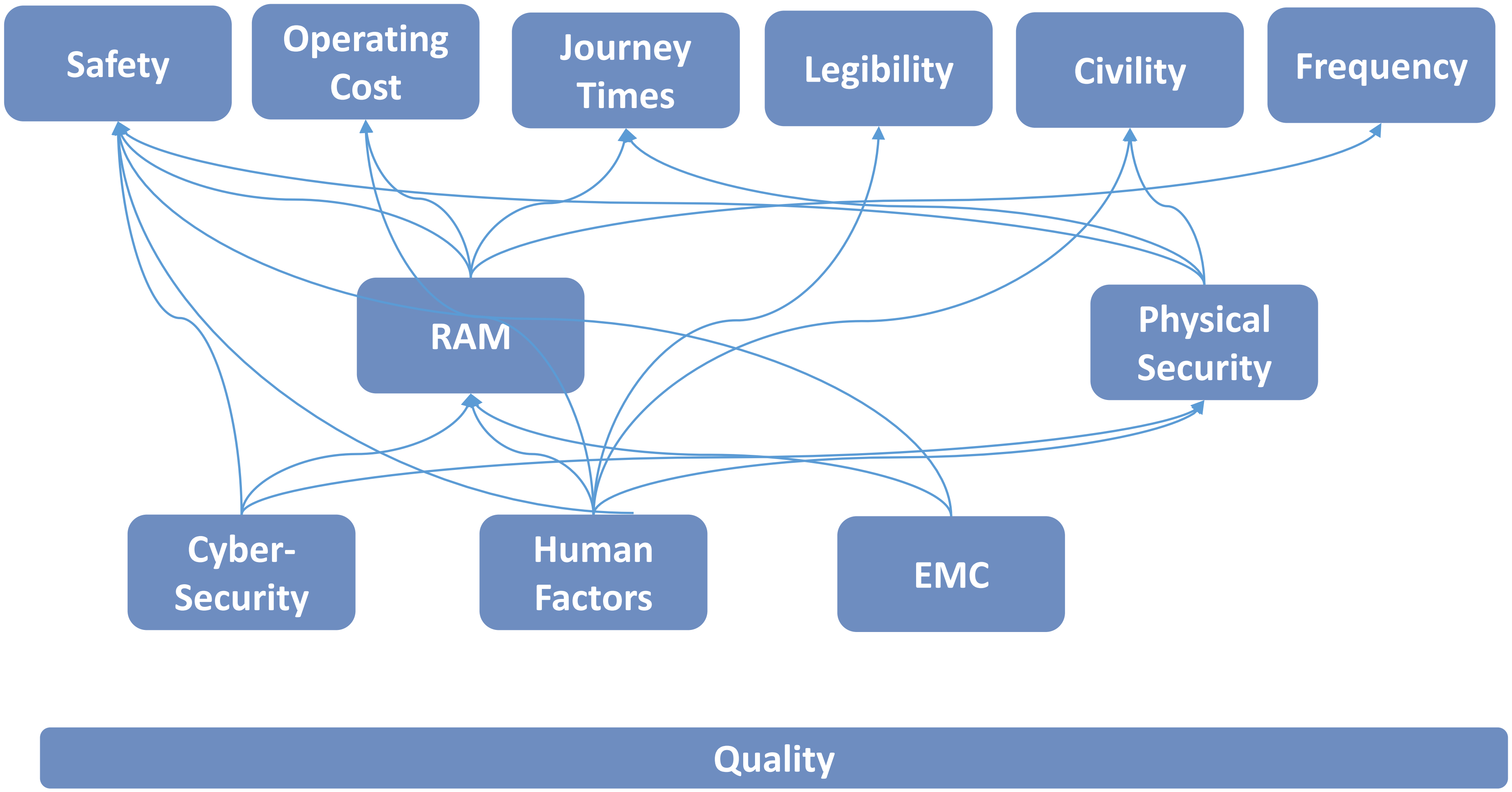
Journey Times

Civility – cleanliness, comfort, security

Service Availability

Operating Costs

A project (large or small) aims to make changes to one or more performance measures of the railway system, whilst maintaining others


Safety
Operating Cost
Journey Times
Legibility
Civility
Frequency
RAM
Physical Security
Cyber-Security
Human Factors
EMC
Quality

System Assurance for Rail Projects

A subset of system engineering activities which provides an argument for claims about one or more properties of the railway as changed by the project.

- Deriving “system” requirements from “business” requirements
- Requires specialist activities (HF, modelling (risk, operations, RAM, etc)
- Tying things together

The tension between breaking things apart and keeping them in context must be dynamically managed throughout the SE process

A project is looking at reducing delays by 20% on a line by duplicating track in certain places and introducing new, more reliable rolling stock.

What is the key system property associated with this project?

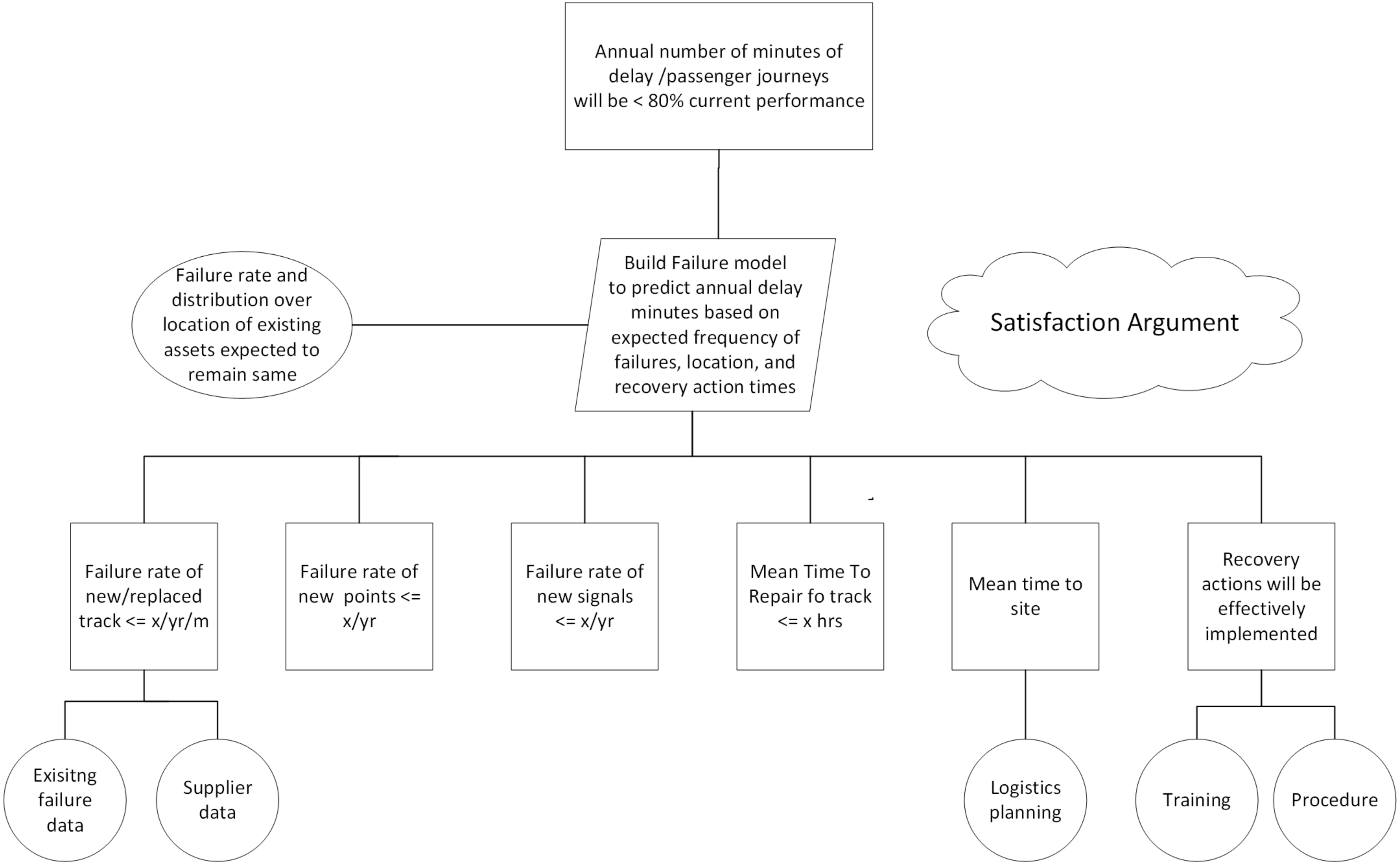
What is the claim?

What is the general structure of the argument for this claim?

What requirements would need to be captured and satisfied for this argument?

What is the claim with respect to safety?

What is the claim with respect to operating costs?



Satisfaction Argument

Annual number of minutes of delay /passenger journeys will be < 80% current performance

Build Failure model to predict annual delay minutes based on expected frequency of failures, location, and recovery action times

Failure rate and distribution over location of existing assets expected to remain same

Failure rate of new/replaced track <= x/yr/m

Failure rate of new points <= x/yr

Failure rate of new signals <= x/yr

Mean Time To Repair fo track <= x hrs

Mean time to site

Recovery actions will be effectively implemented

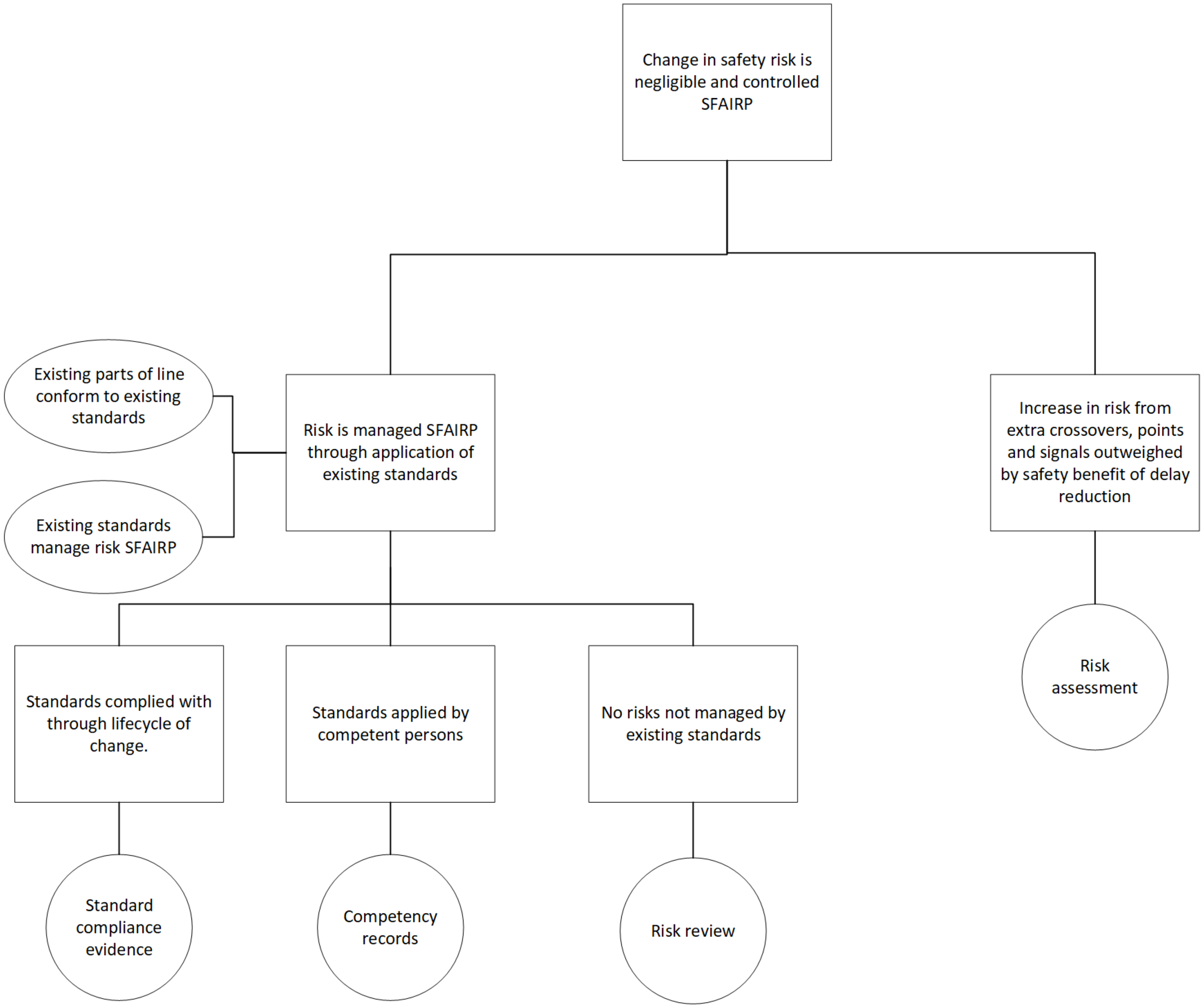
Exisitng failure data

Supplier data

Logistics planning

Training

Procedure


Change in safety risk is negligible and controlled SFAIRP
Existing parts of line conform to existing standards
Existing standards manage risk SFAIRP
Risk is managed SFAIRP through application of existing standards
Increase in risk from extra crossovers, points and signals outweighed by safety benefit of delay reduction
Standards complied with through lifecycle of change.
Standards applied by competent persons
No risks not managed by existing standards
Risk assessment
Standard compliance evidence
Competency records
Risk review

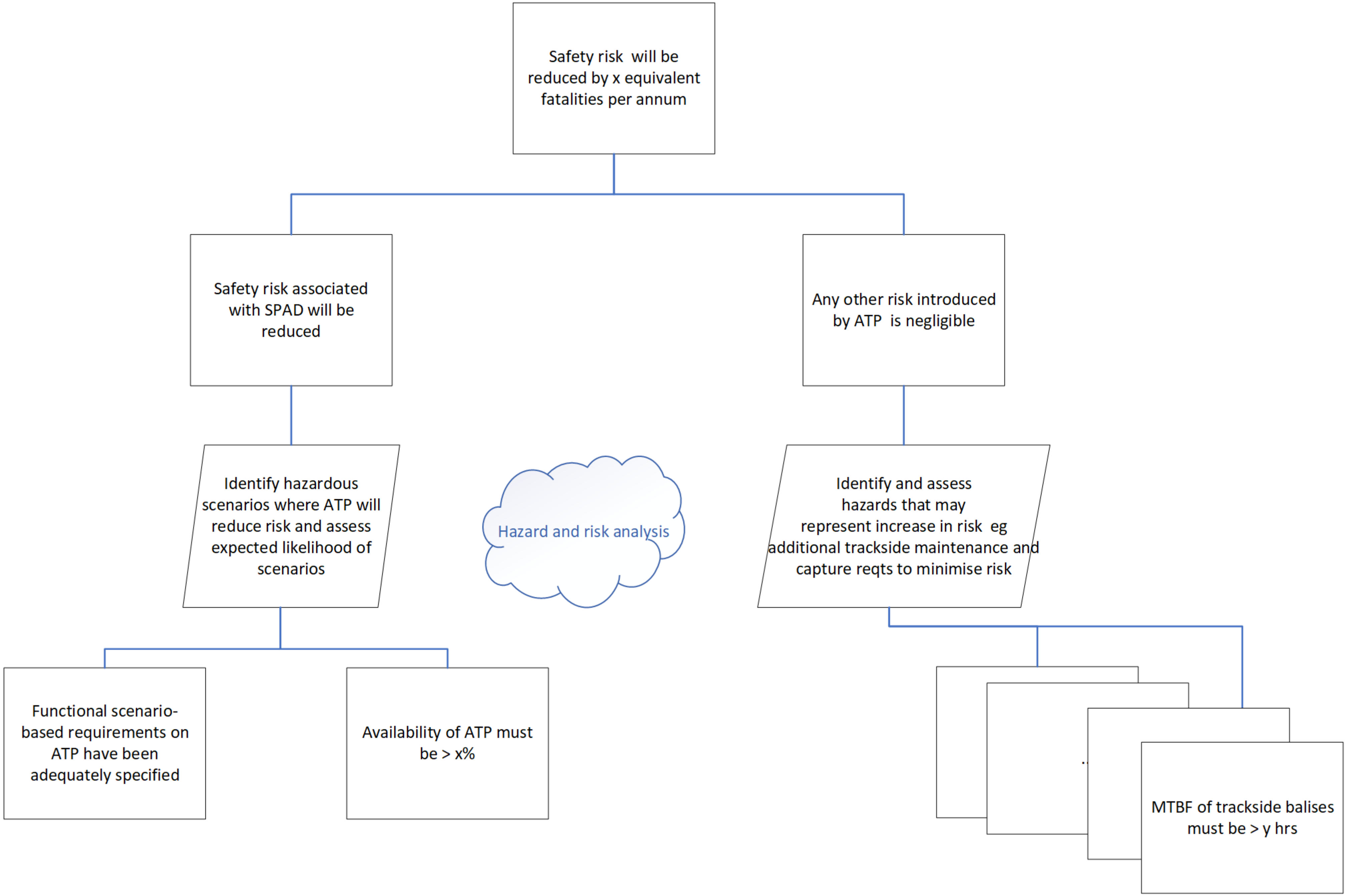
A project is looking at introducing a new Automatic Train Protection system to reduce risk associated with Signals Passed at Danger.

What is the key system property associated with this project?

What is the claim?

What is the general structure of the argument for this claim?

What requirements would need to be captured and satisfied as evidence for this argument?



Safety risk will be reduced by x equivalent fatalities per annum

Safety risk associated with SPAD will be reduced

Any other risk introduced by ATP is negligible

Identify hazardous scenarios where ATP will reduce risk and assess expected likelihood of scenarios

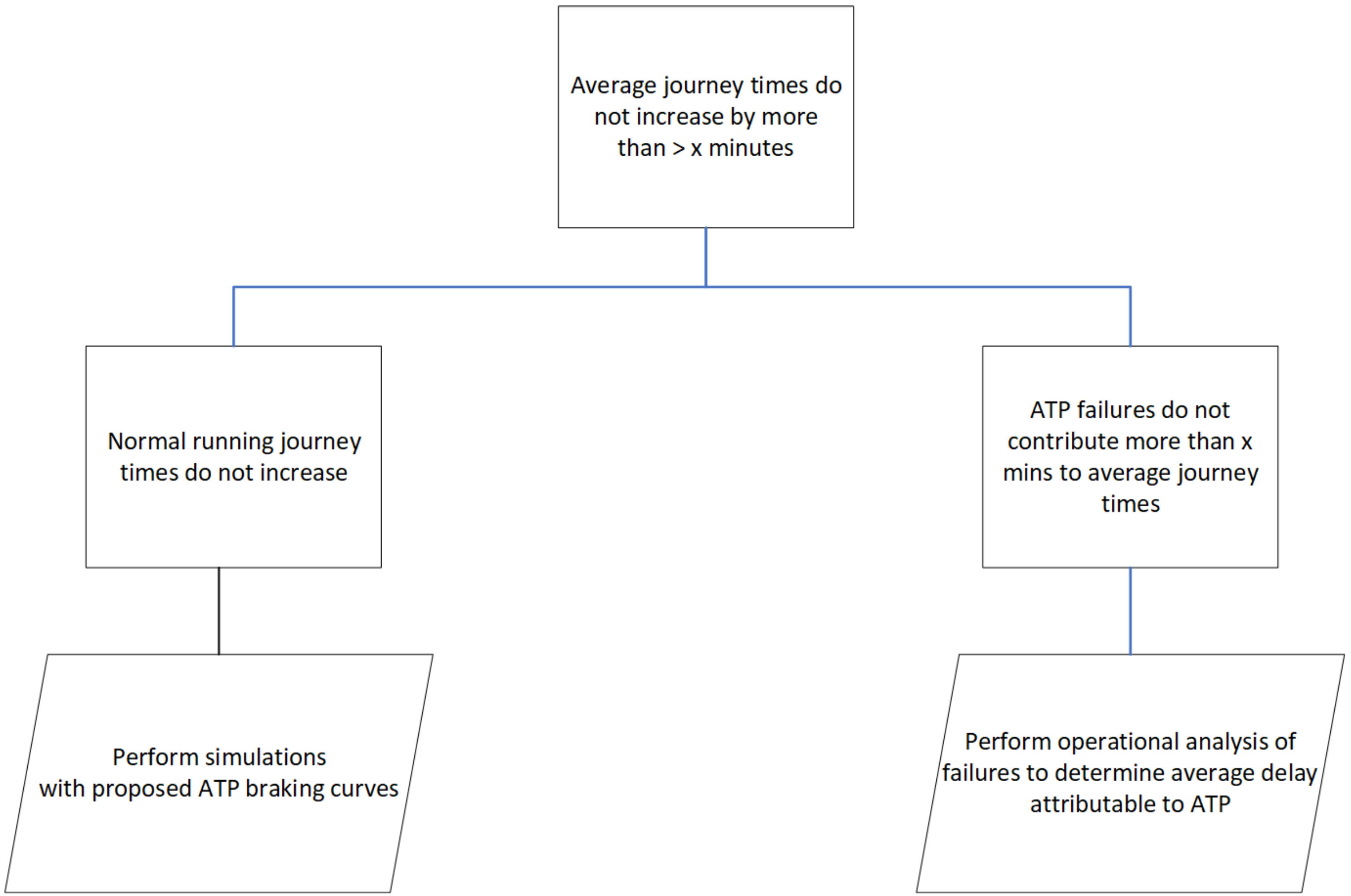
Hazard and risk analysis

Identify and assess hazards that may represent increase in risk eg additional trackside maintenance and capture reqts to minimise risk

Functional scenario-based requirements on ATP have been adequately specified

Availability of ATP must be > x%

MTBF of trackside balises must be > y hrs



Average journey times do not increase by more than > x minutes

Normal running journey times do not increase

ATP failures do not contribute more than x mins to average journey times

Perform simulations with proposed ATP braking curves

Perform operational analysis of failures to determine average delay attributable to ATP

Is the relationship with lower level requirements specifications and performance requirements/goals (satisfaction argument) typically well captured and maintained?

Would the use of graphical arguments help with this?

Would it help “assurance” of the desired performance?