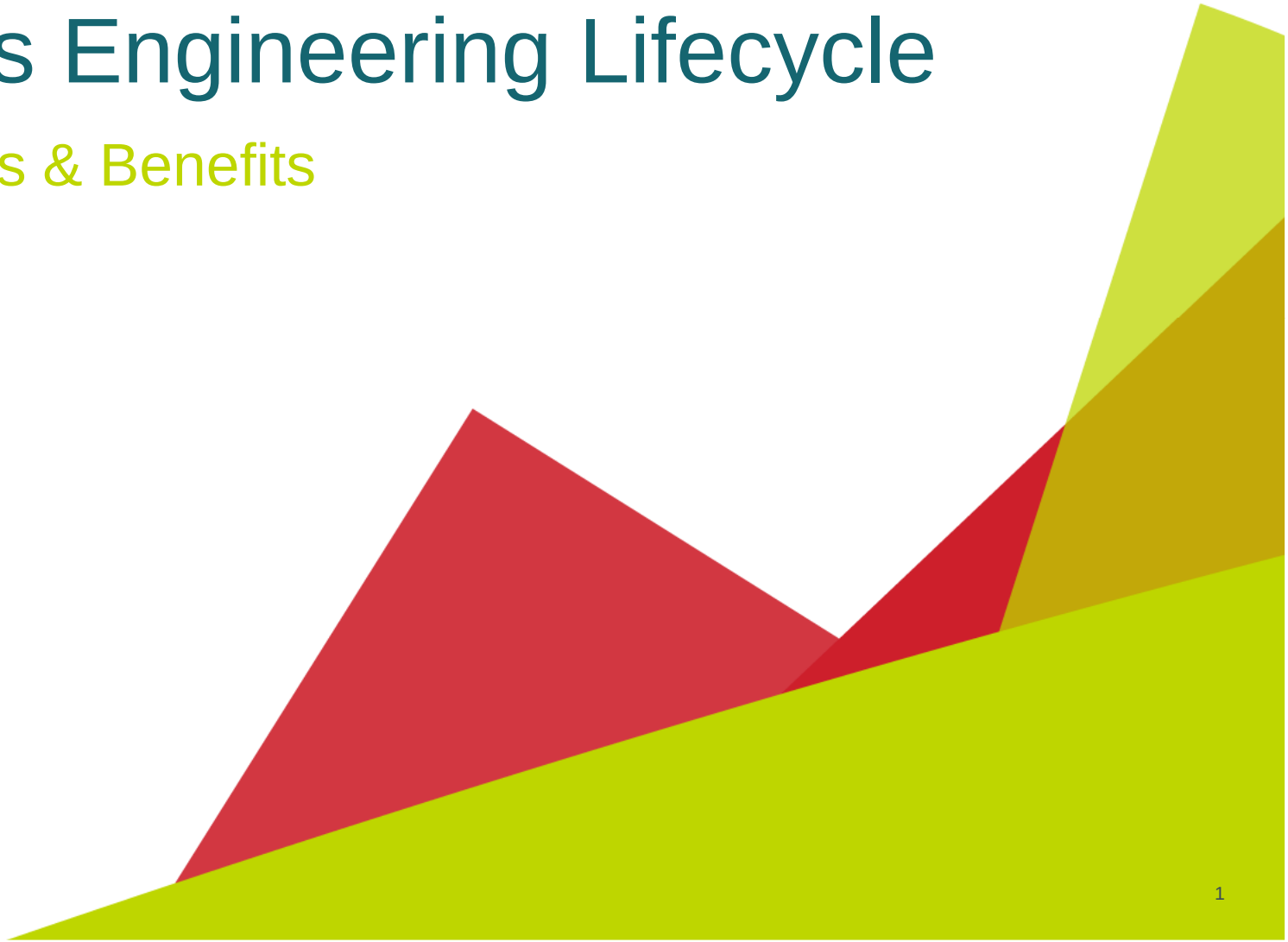
ATKINS

Systems Assurance within the Systems Engineering Lifecycle

Key Lessons & Benefits

Rob Scarbro

12th February 2013



Plan Design Enable

Introduction

ATKINS

- *Overview of Systems Assurance across a Project Life-Cycle*
- *Key objectives, activities and outcomes for:*
  - *Concept / Feasibility*
  - *Detailed Design*
  - *Construction / Test & Commissioning*
- *Summary of key benefits*

Overview of Systems Assurance

Overview of Systems Assurance

ATKINS

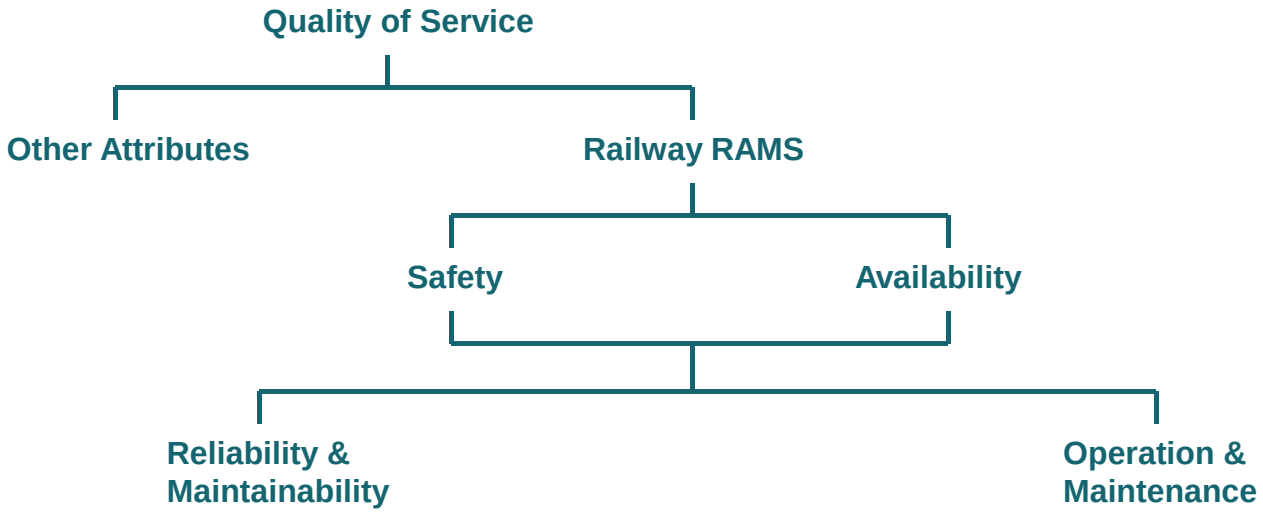
Area of Focus:

Structured and systematic approach to ensuring the requirements related to reliability, availability, maintainability and safety.

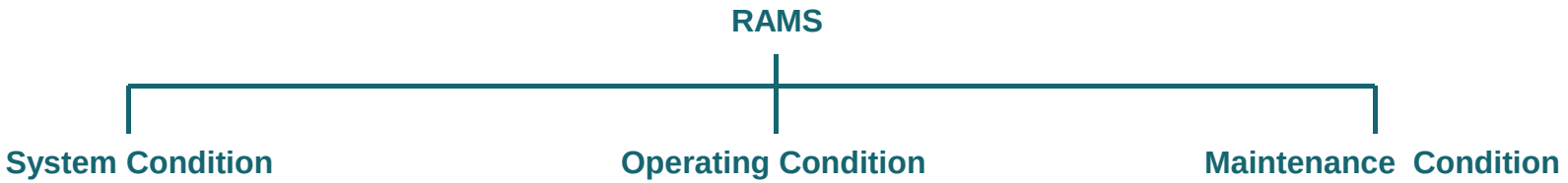
Drivers for Systems Assurance:

- **Work Health and Safety Act 2011 – Including Codes of Practice**
- **Rail Safety National Law**
- *Ensure Safety 'So Far As Is Reasonably Practicable'*
- **EN 50126:1999** – Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
- **AS 4292** – Rail Safety Management
- **YB4** Yellow Book (withdrawn)

Systems Assurance Requirements



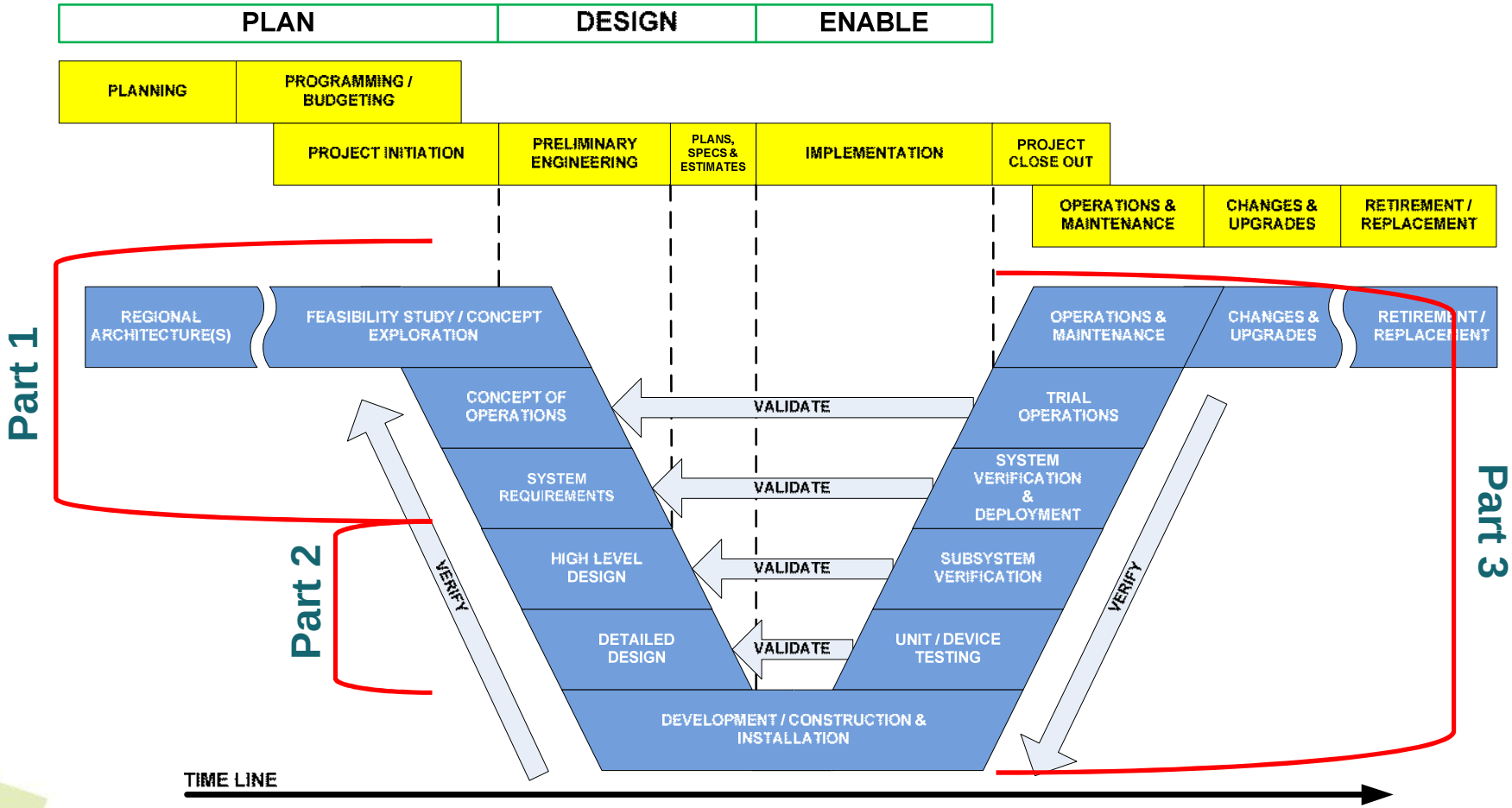
Influence on RAMS



The means used to achieve RAMS requirements are based on the concept of taking precautions to minimise the possibility of ane vent occurring as a result of an error during the lifecycle phases. Precaution is a combination of:

- Prevention: Concerned with lowering the probability of the impairment.
- Protection: Concerned with lowering the severity of the consequences of the impairment.

Systems Assurance Across the Systems Life Cycle



Part 1 Feasibility / Concept

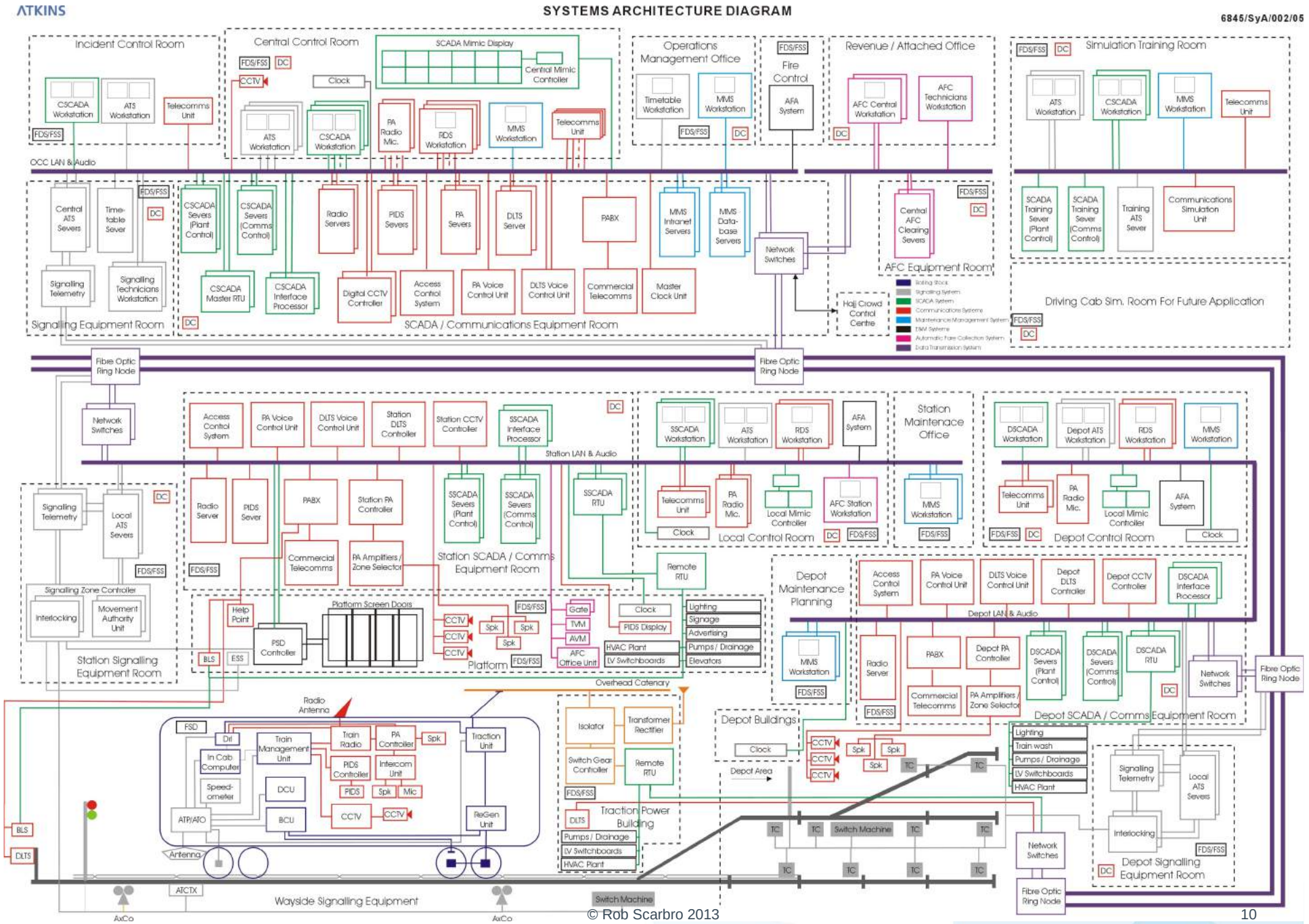
Key Objectives for Feasibility / Concept Phase

ATKINS

- ***Development of scope and context of project***
- *Development of Business Requirements*
- *Sufficient activities to consider options to support planning and business case costing*
- *Identify Key Stakeholders and interfaces*
- ***Develop requirements to enable contracts to be established***
- *Clear, unambiguous requirements (including High Level RAMS requirements)*
- *Aim to deliver options which will not place unacceptable constraints on the delivery entities*

Key Objectives for Feasibility / Concept Phase

- ***Define Interfaces***
- *Understand how the systems will all interact and integrate*
- *Identify the Safety & Performance impact across interfaces*
- *Identify Key Stakeholders*
- ***Understand Functionality***
- *Develop Operations and Maintenance Concepts*
- *Early understanding of functions to identify safety & performance critical functions*
- *Focus on where effort should be e.g. critical areas of the design*
- *Clearly understand the limits of the operating environment the system will be intended to work*

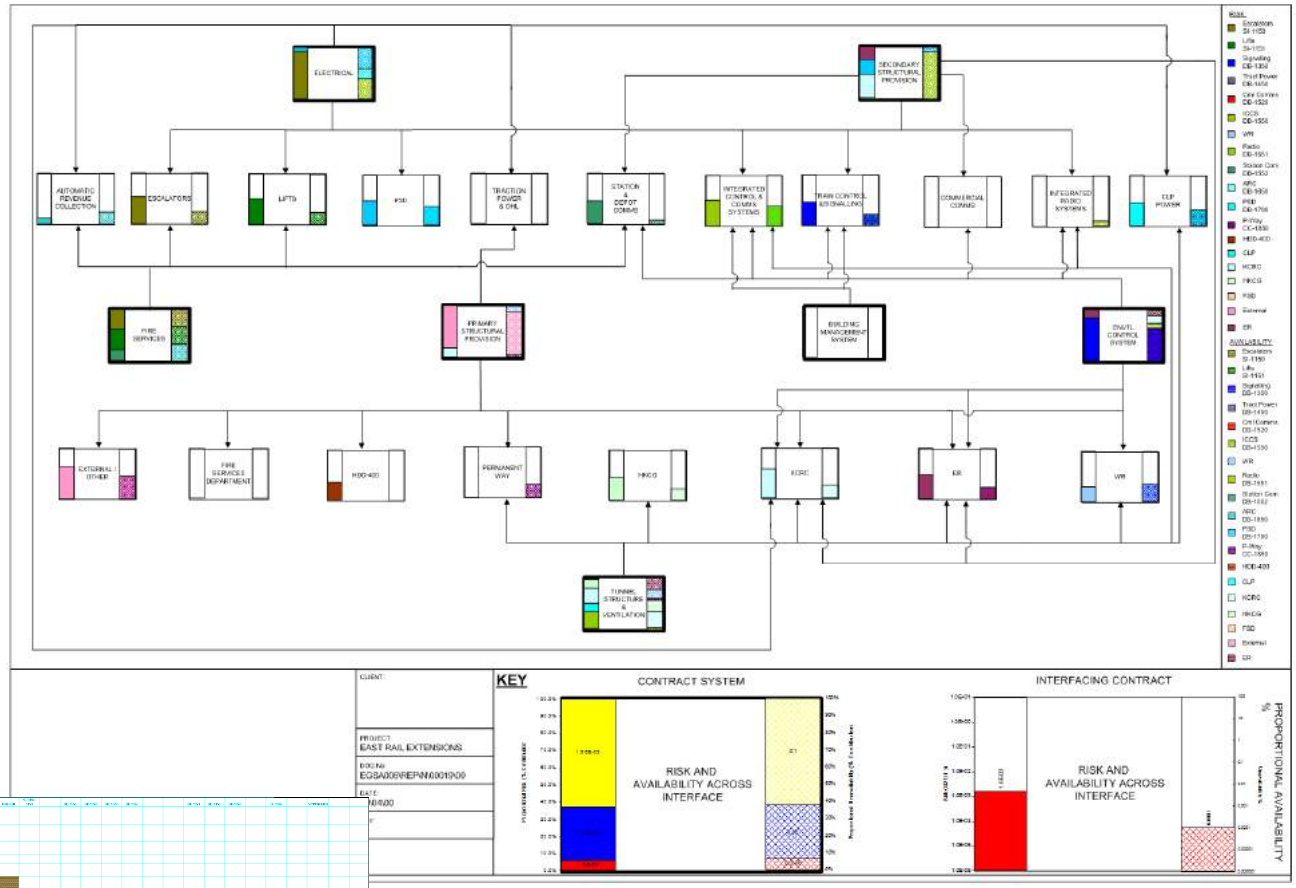


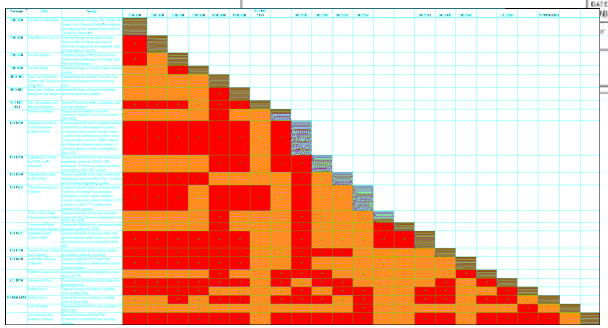
Key Activities during this Phase

ATKINS

- *RAM*
- *High Level RAM requirements*
- *Understanding of current network performance and key impacts on performance (Passengers, Fixed & Moving Assets)*
- *Defining requirements which are clear, measurable, achievable by the contractor*
- *Meaningful apportionment of Network level RAM requirements to the system under consideration*
- *Options analysis to inform RAMS and through life cost requirements*
- *Systems Safety*
- *High Level Safety Requirements – Legal Compliance, SMS, Top Level Safety Requirements*
- *Identification and assignment of interface safety requirements*
- *Preliminary Hazard Analysis – Focus on novel to project, innovative, non-standard NOT what is already well known and understood*
- *RAMS input into Options Development is essential, as the decision on options potentially become constraints to subsequent contractors,* ***so must be demonstrable as considering safety SFAIRP***

Interface Management





Outcomes at Concept / Feasibility

ATKINS

- Structured, apportioned, measurable and achievable RAMS requirements
- Objective evidence of a structured options process considering all risk associated with options
- Safety Assurance of the 'Concept Design' – Demonstrating that decisions have not constrained the ability to manage safety SFAIRP
- Operations, Maintenance and Through Life Concepts and Requirements

Design Activities

Key objectives during Design Phase

ATKINS

- *Clear and articulate road map to the achievement of RAMS in the detailed design development*
  - *Systems Assurance integral to design activities*
- *Identify and capture objective evidence of a systematic and structured set of design activities, which:*
  - *Systematically Identify Hazards and design controls to eliminate, or engineer controls to manage safety SFAIRP;*
  - *Deliver an assured design which assures the optimal outcome for its **end purpose** to achieve the optimal solution to meet the RAMS requirements at the best Through Life Cost*
- *Identify what success looks like (Pass/Fail criteria) for construction / manufacture (ITPs, tolerances, operating limits)*

Key Activities during this Phase

ATKINS

- ***RAM***
- *RAM Requirements and Analysis*
- *FMECA*
- *Corrective / Preventative Maintenance*
- *RMDT Planning inc FRACAS*
- ***Systems Safety***
- *Detailed Hazard Analysis*
- *Fault Tree Analysis / Event Tree Analysis*
- *Safety Case Development (inc. GSN Safety Argument)*
- *Early identification / acceptance in principal of proposed operational and maintenance controls (assessment against O&M Concepts)*

Outcomes at Design

ATKINS

- Design demonstration that if built as designed, the RAMS requirements will be achieved in the operating environment (normal and degraded)
- Design Safety Argument (or Safety Case) demonstrating that in Principal the Design has managed risk So Far As Is Reasonably Practicable
- Inspection and Test Plans (ITPs) or equivalent developed to demonstrate how requirements will be demonstrated during construction / manufacture phase

Taiwan High Speed

ATKINS

SYSTEMS ASSURANCE OBJECTIVE FOR THE PROJECT

Support the Core Systems certification through a Systems Assurance Programme compliant with EN 50126 and achieving the contractual RAMS requirements

STATUS OF RAMS PROGRAMME AT PRELIMINARY DESIGN

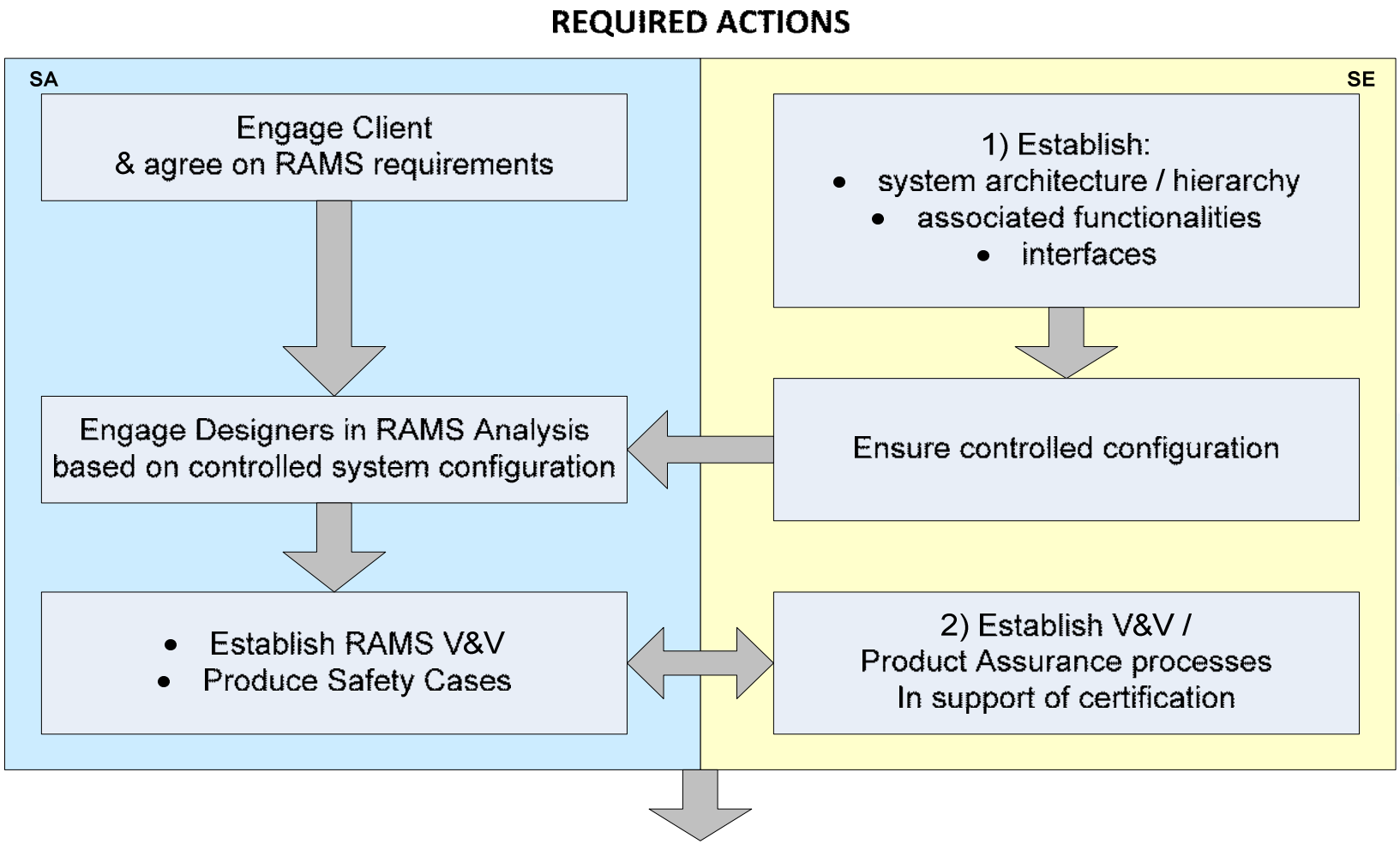
SA

RAMS Programme approved by Client without clear agreement on the interpretation of RAMS requirements

SE

1) Poor definition of systems architecture & functionalities due to insufficient management of System Engineering
2) Poor definition of V&V process

Taiwan High Speed



Taiwan High Speed

ATKINS

LESSON LEARNED - KEY FACTORS TO DELIVER INTEGRATED SYSTEMS ASSURANCE

- Clear understanding of Systems Assurance requirements, agreed upfront with all stakeholders
- Establish and maintain sound SE and SA processes to ensure that:
  a) designers are pro-actively engaged with RAMS delivery
  b) RAMS is concurrent with design through effective management of system configuration and interfaces
  c) evidence in support of safety demonstration for the system certification is objective, traceable and auditable.

Manufacturing / Construction

Key Objectives for the Construction / Commissioning & Handover phase

ATKINS

- **Construction Assurance**
- The ‘As Built’ meets the Design Intent
- Requirements and specifications are verified and validated
- Verification and Validation of RAMS Requirements
- Engineering Change Management effectively manages configuration change from the design
- Provision of structured, supported assurance case with physical and procedural objective evidence which supports the systems being accepted into operations and maintenance
- Development of Operations and Maintenance Manuals and Operational Readiness

Key Systems Assurance activities through Manufacturing/Construction

ATKINS

Build / Manufacture Assurance

- Quality assurance of assets
- Sub-System Testing – Factory Acceptance
- Management of changes, re-assessment of RAMS, design changes to support change
- Established FRACAS Systems, to records failures and rectify defects
- Verification and Validation of RAMS Requirements
- Safety Requirements Verification & Validation
  - Looking for objective evidence
  - Should be no doubt what the evidence of a requirement is
  - 100% V&V of Safety Requirements, traced to explicit Safety Controls within the Hazard Log

Summary

ATKINS

- Top down approach understanding the network, systems and deriving RAMS requirements that lay the foundation for successful delivery
- Engage RAMS from the outset of a project
- RAMS activities are integrated engineering activities and support the design and construction delivering the required safety and integrity
- Start with the end in mind and identify how the next phase will demonstrate requirements are met (ITPs etc)
- Collation of structured objective evidence in a manner that enables an argument to be made of the overall assurance

Any Questions?

ATKINS

ATKINS

Plan Design Enable