CPNI

Centre for the Protection of National Infrastructure

WORKED EXAMPLE: REQUIREMENTS AND POLICIES ASSURANCE CASE

Scenario-based guidance to developing a security-informed safety case analysing security and safety policies and requirements.

CONTENTS

FIGURES

TABLES

01. INTRODUCTION

This document provides a worked example of a requirements and policy assurance case analysing the security and safety policies and requirements. It can be used as a practical guide to illustrate the process of developing the first part of the security-informed safety cases using a combined approach as set out in 'Combined Approach to Developing Security-Informed Safety Assurance'.

As prerequisites, this guidance relies on good knowledge of the Claims, Arguments and Evidence (CAE) concepts and their application to the development of assurance cases. It also assumes the reader is familiar with the other guides available on the CAE approach available on the CPNI website.

The focus of this guidance is on the requirements and policies layer (L0) described in 'Combined Approach to Developing Security-Informed Safety Assurance'. The architectural (L1) and implementation (L2) layers are the focus of 'Worked example: Architecture and Implementation Assurance Case'.

L0 is the first stage of analysis and considers the highest level of abstraction where the system represents its requirements, and where the safety and security policies are scrutinised to identify any conflicts and analyse any trade-offs. Addressing requirements and policy issues at this initial stage, early in the system lifecycle, can bring significant returns on investment and help to avoid bigger problems and much higher costs in the future.

The development of the requirements and policies (L0) assurance case is done by working through the first three steps of the cyber security risk assessment process set out in 'Risk Assessment Process' guidance, specifically:

Step 1 – Establish system context and scope of assessment

Step 2 – Configure risk assessment

Step 3 – Analyse policy interactions

The combination of the layered assurance and cyber security risk assessment process facilitates a thorough analysis of the system, helping to develop a good understanding of the technical detail and identify issues that may need to be addressed.

The guidance document illustrates the practical application of the approach to a case study of a transport advisory system. It describes the scope and boundaries of the system, outlines the results for each of the cyber security risk assessment steps, and demonstrates the construction of the L0 assurance case. The example has been anonymised to ensure confidentiality of the actual system and organisation.

The guidance is aimed at experienced practitioners who have understanding of safety and security aspects but would like to see a real-world example on how the security-informed safety cases are developed in practice.

02. SIGNPOSTING

This is the first example-based guide in our stack of resources for security-informed safety assurance. Figure 1 below shows its location in the set of guides (highlighted in red).

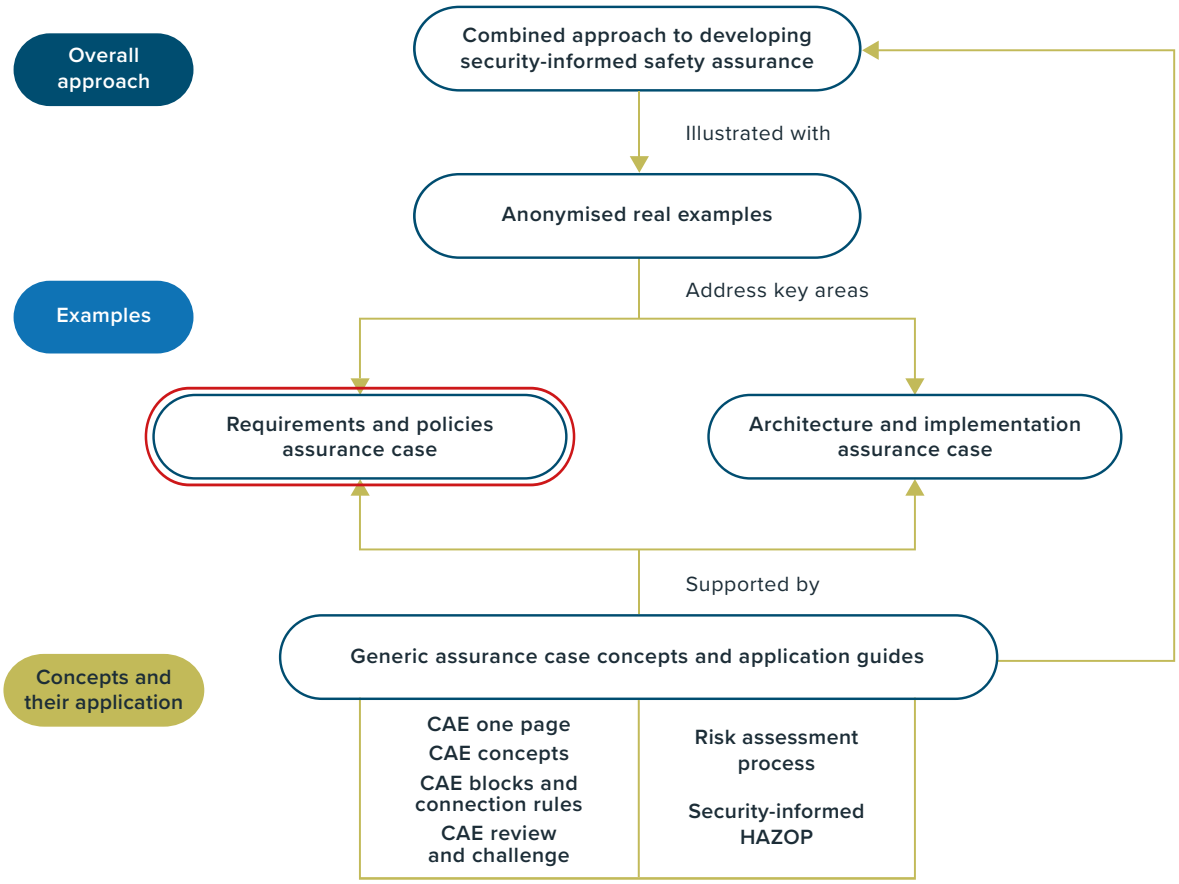

Figure 1: Location of this guide in the set of resources

03.
CASE STUDY ANALYSIS

In this section the application of the first three steps of the risk assessment methodology and the construction of the L0 case for the transport advisory system (TRAS) are discussed in detail.

3.1 STEP 1 – TRAS SYSTEM CONTEXT AND SCOPE OF ASSESSMENT

The example TRAS system was an upgrade to an advisory system used in the transport industry. It provides functions for maintenance management recording and asset data. It is a new web-based system migrating most functionality from the existing 'legacy' mainframe systems applications but still maintaining an interface to a few functions that are not migrated. New functionality will be added, including improvements to maintenance planning. Improvements will also be made to interfacing with other applications, and to data analysis and reporting.

The user experience will be web-based with a menu-driven navigation system, with no local software required other than a web browser and local system interfaces. Users will be able to generate reports via a virtual private network (VPN) client connection to the TRAS infrastructure. This will allow users to publish reports to the Reports Server that is available for all users.

In addition to redeveloping the existing elements, a number of new elements and functionality will be implemented. A new Business Intelligence (BI) solution will allow tailored analysis of the TRAS data, including support for industry key performance indicators.

Most of the delivered areas of functionality including standard reporting, excluding the BI ad hoc analysis, will be accessible through an Internet portal with a new web-based graphical user interface, delivering a similar look and feel across the TRAS application.

The TRAS access control mechanisms will ensure that all parties with an interest in specific items can access the information they need, whilst restricting read and write access to sensitive data to authorised users only. Use of common coding systems and interface standards ensures a common understanding of the data.

This case study focuses on the TRAS functional scope illustrated in Figure 2. External systems interfacing with TRAS are out of scope of the case study and would require a separate analysis.

03.
CASE STUDY ANALYSIS

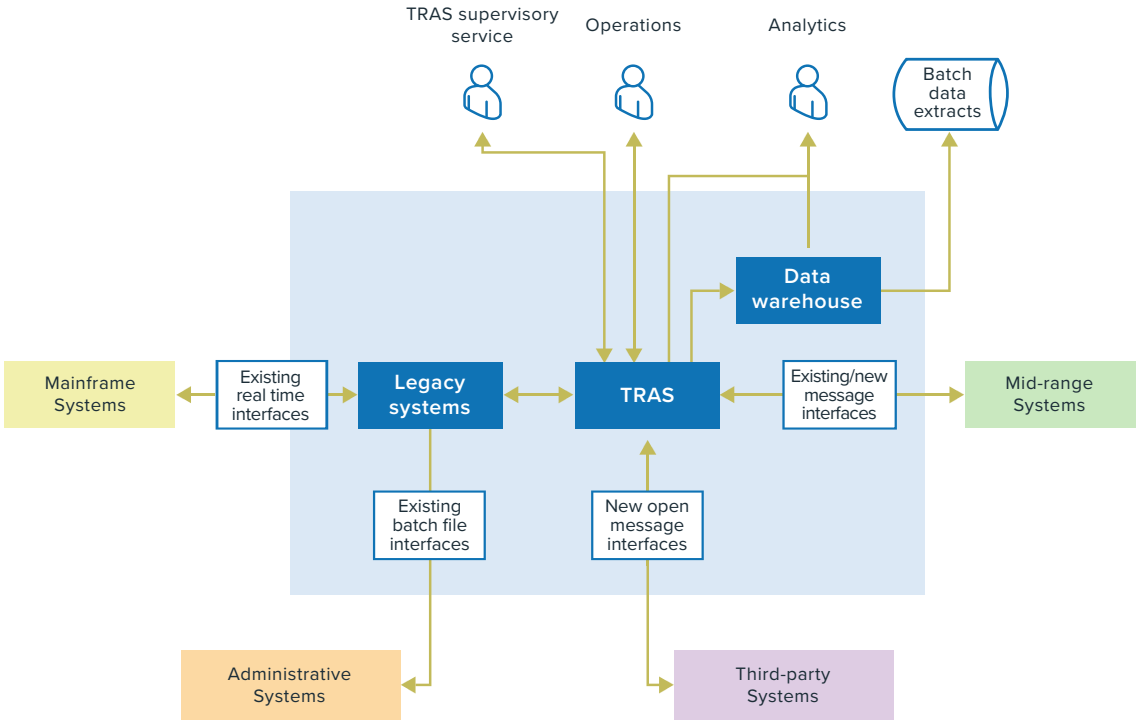

Figure 2: TRAS context diagram

The TRAS database is hosted by one of the global hosting companies on a Microsoft SQL server and located in a European data centre.

Within this architecture, the core business service components are delivered in a resilient manner, through the use of clustering approaches in order to ensure that the business service that they deliver would continue if one of the component elements were to suffer a failure.

From the data it contains and the functionality of TRAS, a set of Material Safety Uses (MSU) was produced that defines, as the name suggests, the safety relevant uses for TRAS and the rationale. The MSU report gives clear guidance about who is using data stored in TRAS and for what purposes, whether they have a safety relevance, and what might be the potential consequences if the MSU failed.

The TRAS system has several other requirements that have to be taken into account:

- Service-level requirements ask for an availability of the service of 99.67% with defined/allowed maintenance times that have to be announced to the users;
- integrity requirements are not defined;
- security measures that are to be in place:
    - o authentication for secure VPN for external users and for access to server;
    - o antivirus;
    - o firewalls;
    - o backups (different plans are in place);
    - o annual penetration testing;
    - o patching; and
    - o monitoring of metrics (server CPU, memory and availability);
- access requirements from and to TRAS by other systems as well as users:
    - o remote desktop: VPN;
    - o web interface (browser): https, tcp/ip;
    - o Third-party maintenance: https, tcp/ip; and
    - o existing mainframe

In terms of the system boundaries, there are hazards in the wider transport system (the negation of the MSU) that could lead to accidents and there are hazards with respect to the TRAS system: hazards are potential loss events or states on the boundaries of the system.

03.
CASE STUDY ANALYSIS

3.2 STEP 2 – CONFIGURING RISK ASSESSMENT

At this step, safety documentation for legacy parts of the system has been identified. The TRAS sponsor is leading work to develop a safety case for TRAS.

Based on system criticality and infrastructure, attack capability level C is proposed to be appropriate. This is to be confirmed with Government specialists.

To proceed with the analysis, the system model has been refined and focused to make it at the right level of detail for an effective security-informed risk assessment. The model is provided in Figure 3.

The potential threats/causes (Ca) are identified at the boundary or within TRAS. They might lead to hazardous events or situations (H), which are identified as potential failure possibilities, and are protected by safeguards within TRAS (P) against such a top event happening. However, there must also be barriers that mitigate the consequences (C) of the top event occurring, which would be violations of the MSU. In the wider system, which is not within the scope of this study, the failure of the MSU may lead to hazardous situations on vehicles that are in operation (A).

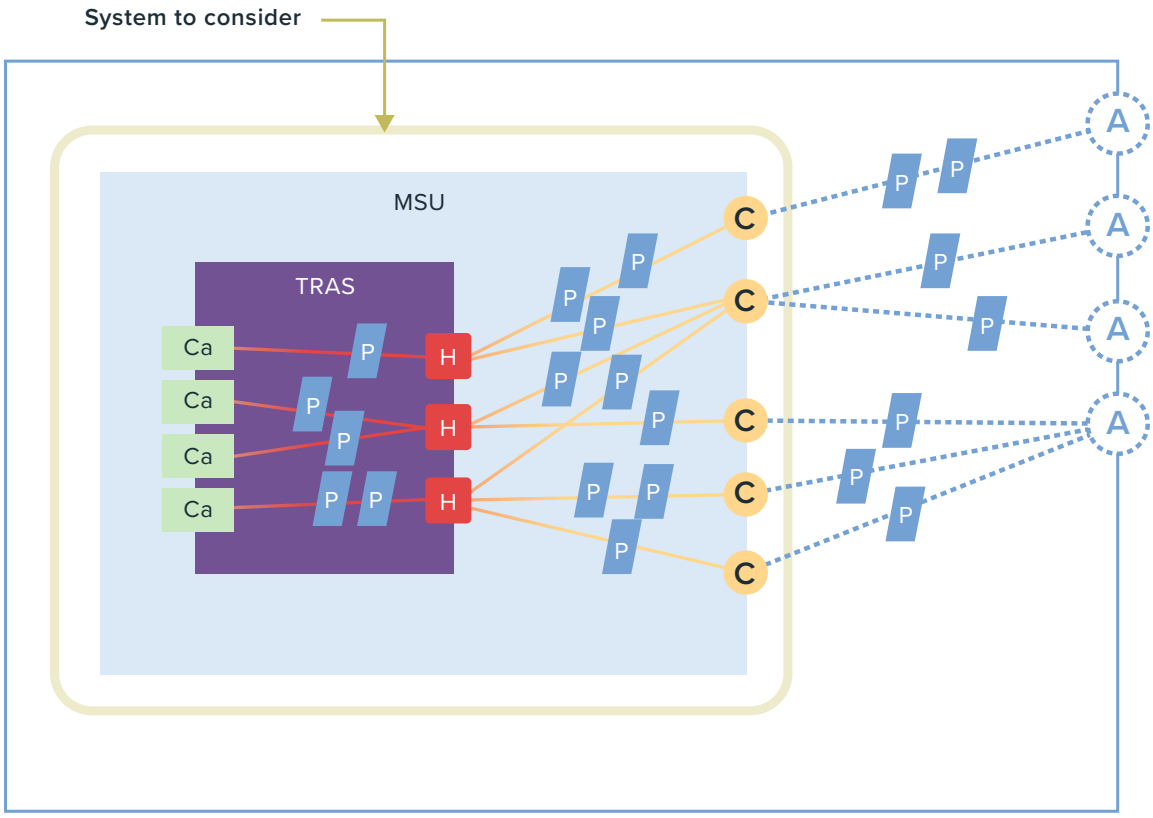

Figure 3: System boundaries that are considered for risk assessment

03.
CASE STUDY ANALYSIS

3.3 STEP 3 – ANALYSIS OF POLICY INTERACTIONS

There can be interactions between the safety requirements and security policies and these should be assessed, at least initially, at L0 (or at Step 3 of the risk engineering process). For TRAS these could concern:

- the use of the system in emergency situations (e.g. following major accident or loss of communications) that might be constrained or hampered by access policies; and
- the need to recover quickly to ensure continuation of service which might conflict with security.

The analysis of interactions was discussed at the initial safety workshop and it was considered that while TRAS might have a role in these issues the tempo of service recovery would not be hampered by the security policies.

Some examples of the policy issues are considered in Table 1 and Table 2 below and are part of the approach defined in the 'Risk Assessment Process' guidance.

In addition, at this stage a range of policies have been identified that may to some extent be defined at L0 but will require detailing and implementing at L1 and L2. Some of these design and implementation policies are considered in Table 2. The details of the L1 and L2 analysis are available in 'Worked example: Architecture and Implementation Assurance Case'.

Policy issue	Activities	Case study
Scope of system, safety case and safety-related functionality	Assess whether system boundary is drawn sufficiently wide, e.g. to include sources of attack, connected systems. Assess whether additional confidentiality claims are needed, e.g. system does not leak information that leads to unacceptable increase in risk of successful attack, system protects confidentiality of assets that have direct information value.	The system boundary has been defined as where the MSUs are identified and the TRAS-hazards on the TRAS boundary.
	Assess the role of the system/service in enabling other systems to be secure – good cyber citizenship.	This was covered at the security-informed Hazop workshop.
	Consider an explicit claim about resilience to emphasise the need for adaptation and recovery in an uncertain world. This will require interactions with the other system owners and their policy setters.	The role of TRAS in resilience was discussed at the security-informed Hazop workshop.

Table 1: Policy checklist example

Design and implementation policies	Application
Policy on which sets of 'critical controls' should be considered or mandated	There is no explicit policy on the "critical controls". The coverage with respect to these should be assessed in L1.
Policy on application of Kerckhoff's principles	None
Policy on applicable standards and guidance	Discussed in Business Requirements and safety case.

Table 2: Design and implementation policies – example

03.
CASE STUDY ANALYSIS

3.4 ASSURANCE CASE AT THE POLICY AND REQUIREMENTS LEVEL

At L0, the system's safety and security requirements are analysed and the claim that they are adequate is assessed by considering both the content and the quality of the requirements. The content analysis is concerned with what is in the requirements and the aim is to ensure the captured set of requirements is valid and complete. The quality analysis is about how the requirements are presented: it needs to be ensured that all the requirements are well-defined with each individual requirement being of good quality (i.e. consistent, unambiguous, atomic, etc.). This expansion is shown in Figure 4.

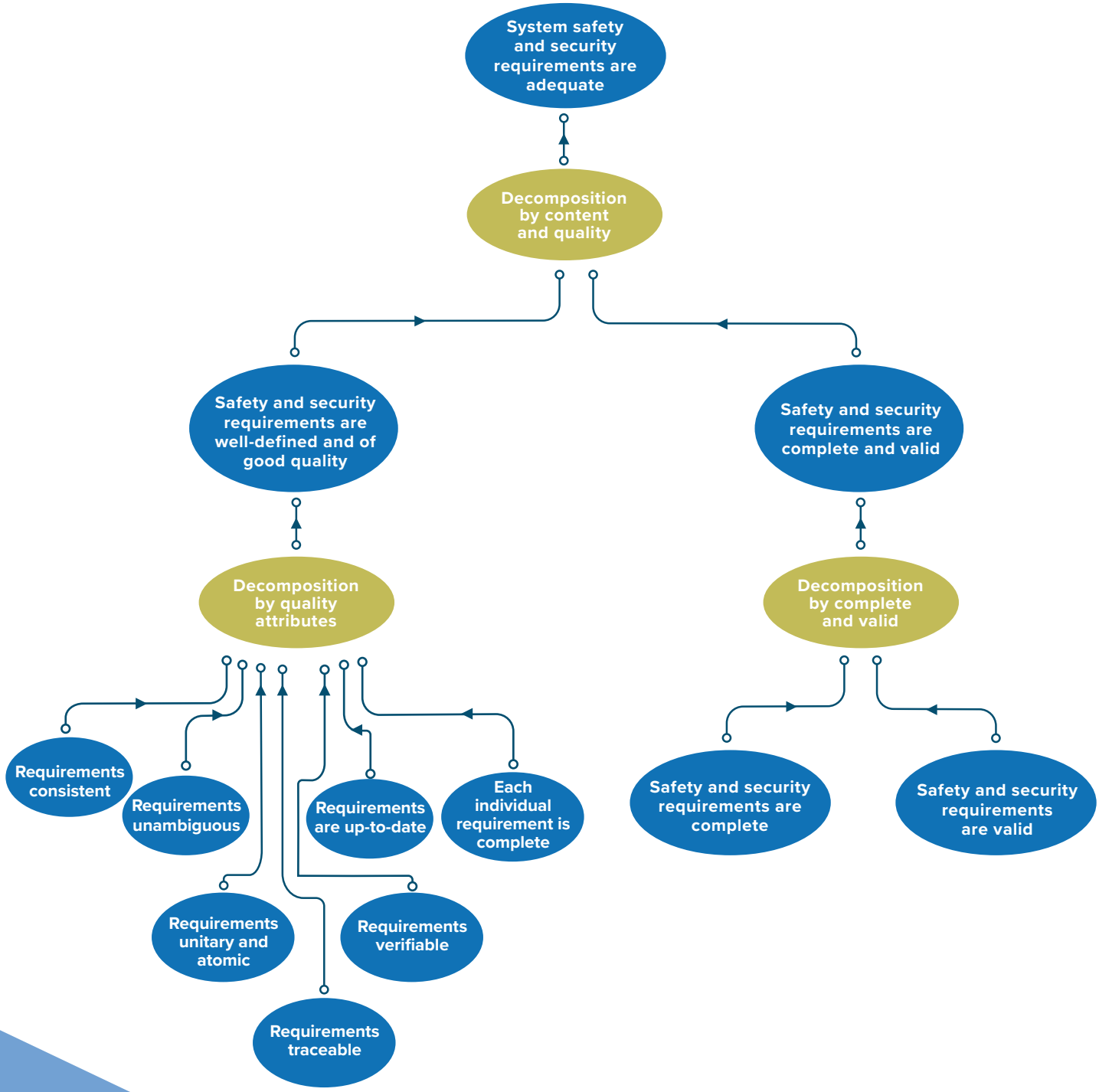

Figure 4: High-level expansion dealing with attributes of good requirements

03.
CASE STUDY ANALYSIS

The left-hand side branch provides a set of claims regarding the quality of requirements, all of which should be supported by the related evidence coming from the analysis.

The right-hand side branch, however, is not likely to be directly supported by the evidence and requires further expansion. To support the subclaim about completeness it is necessary to look into all the various sources that are taken into account when constructing the overall set of security and safety requirements. These normally include safety-related sources (including any existing analyses, e.g. safety cases), security-related analyses, various policies and constraints (including standards and guidelines to be complied with, any particular approach to assurance, etc.).

Additionally, there may be security and safety policies that cannot be applied in isolation. In that case some decisions have to be made about them. it is important to undertake and document a security-informed safety analysis to show that the interaction and trade-offs are satisfactory. The analysis of the policy interactions will be based on the safety requirement and the security policies together with their respective supporting analyses. The expansion is shown in Figure 5.

03.
CASE STUDY ANALYSIS

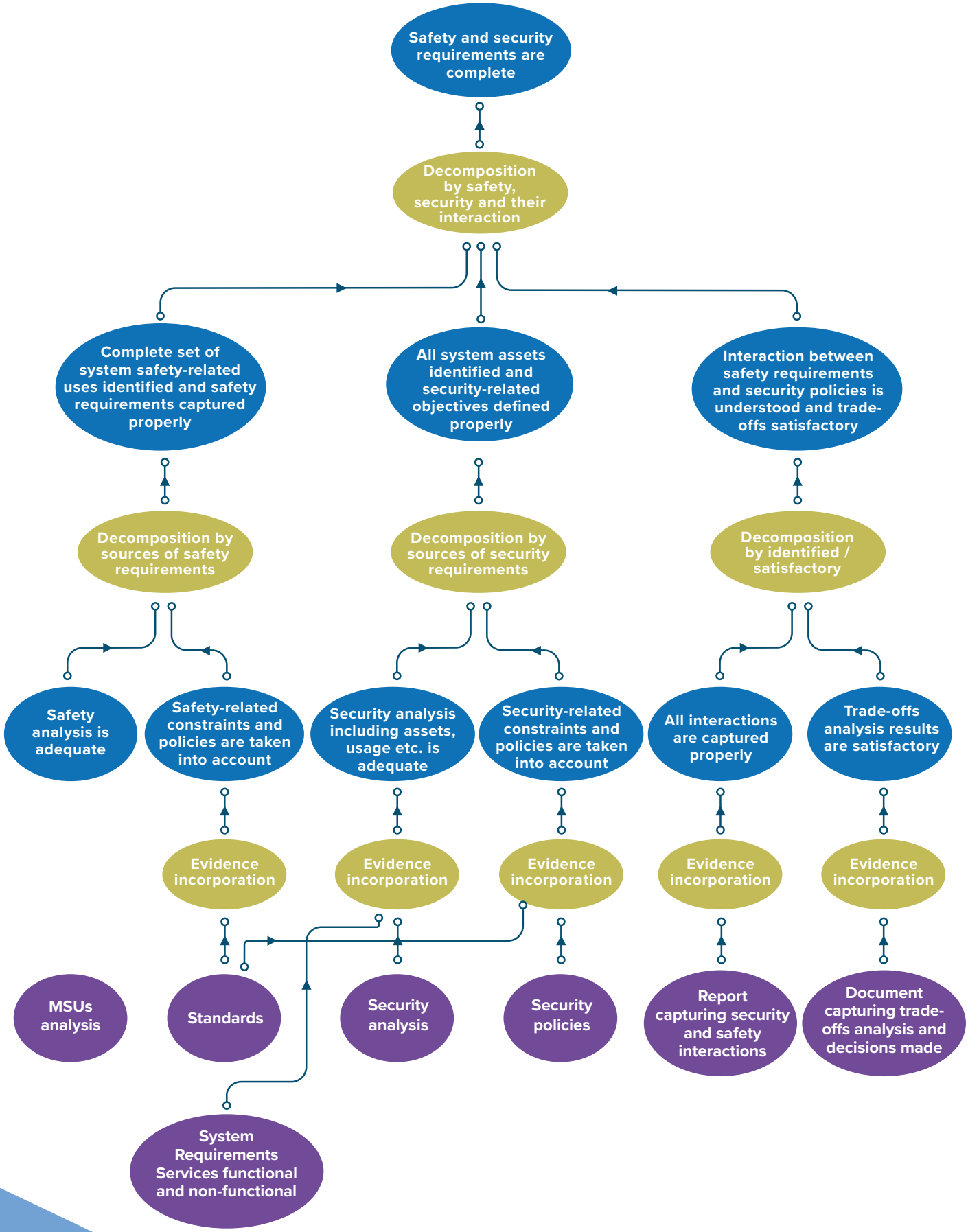

Figure 5: Case structure dealing with various sources of safety and security requirements

03.
CASE STUDY ANALYSIS

The validity of requirements needs to be thoroughly considered by expanding the claim in a more detailed case. Valid in this context means that the safety requirements reduce risks to tolerable and 'as low as reasonably practicable' (ALARP). The first step is to defining the claim more precisely using a Concretion block (see 'CAE Blocks and Connection Rules'). The case can be expanded further into subclaims about the requirements covering tolerability of the risks from equipment and ALARP demonstration requirements with respect to design and operation. This expansion is shown in Figure 6. Figure 7 shows the decomposition by property of the reduced risk.

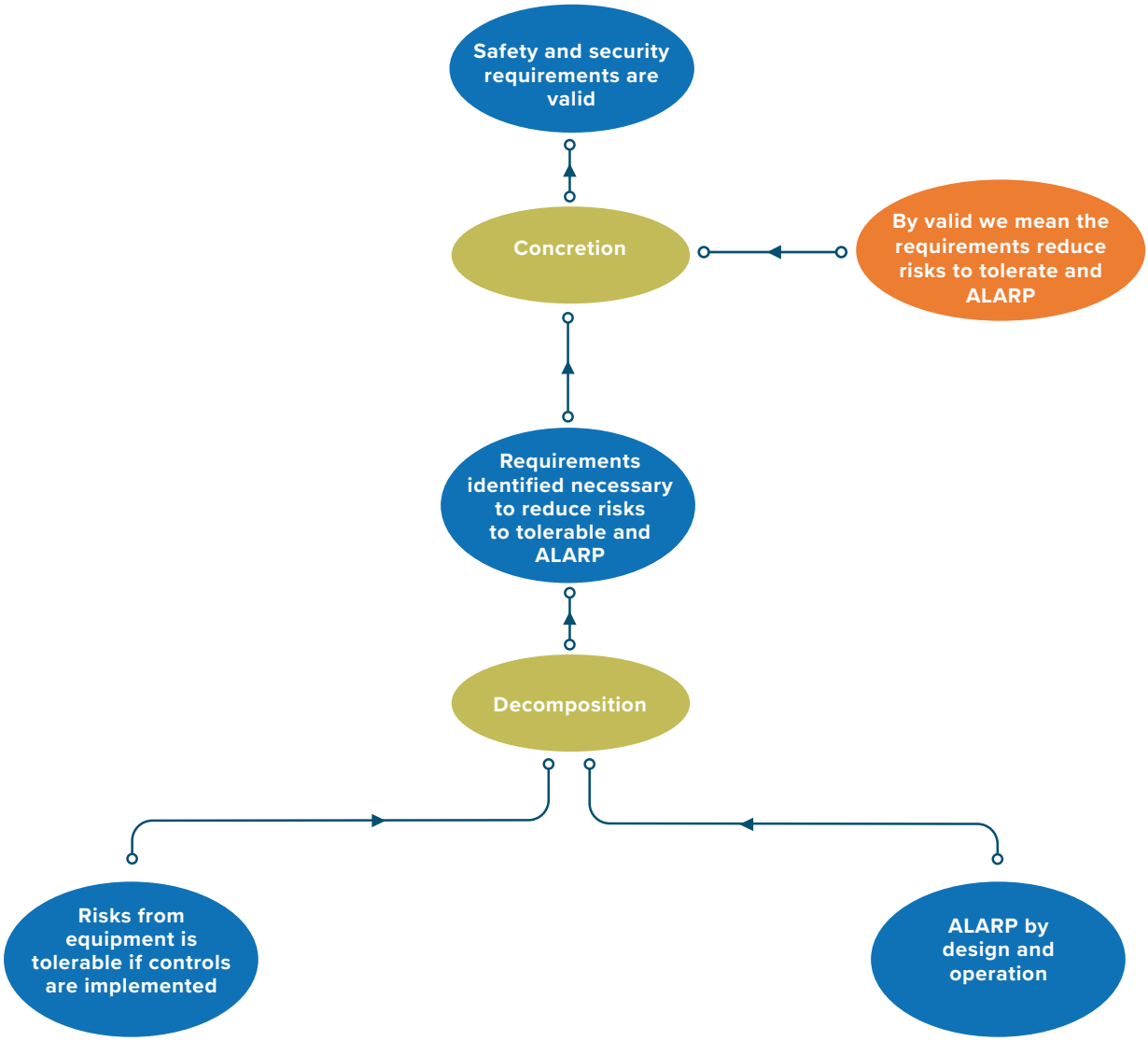

Figure 6: Validity of requirements high-level claims

03.
CASE STUDY ANALYSIS

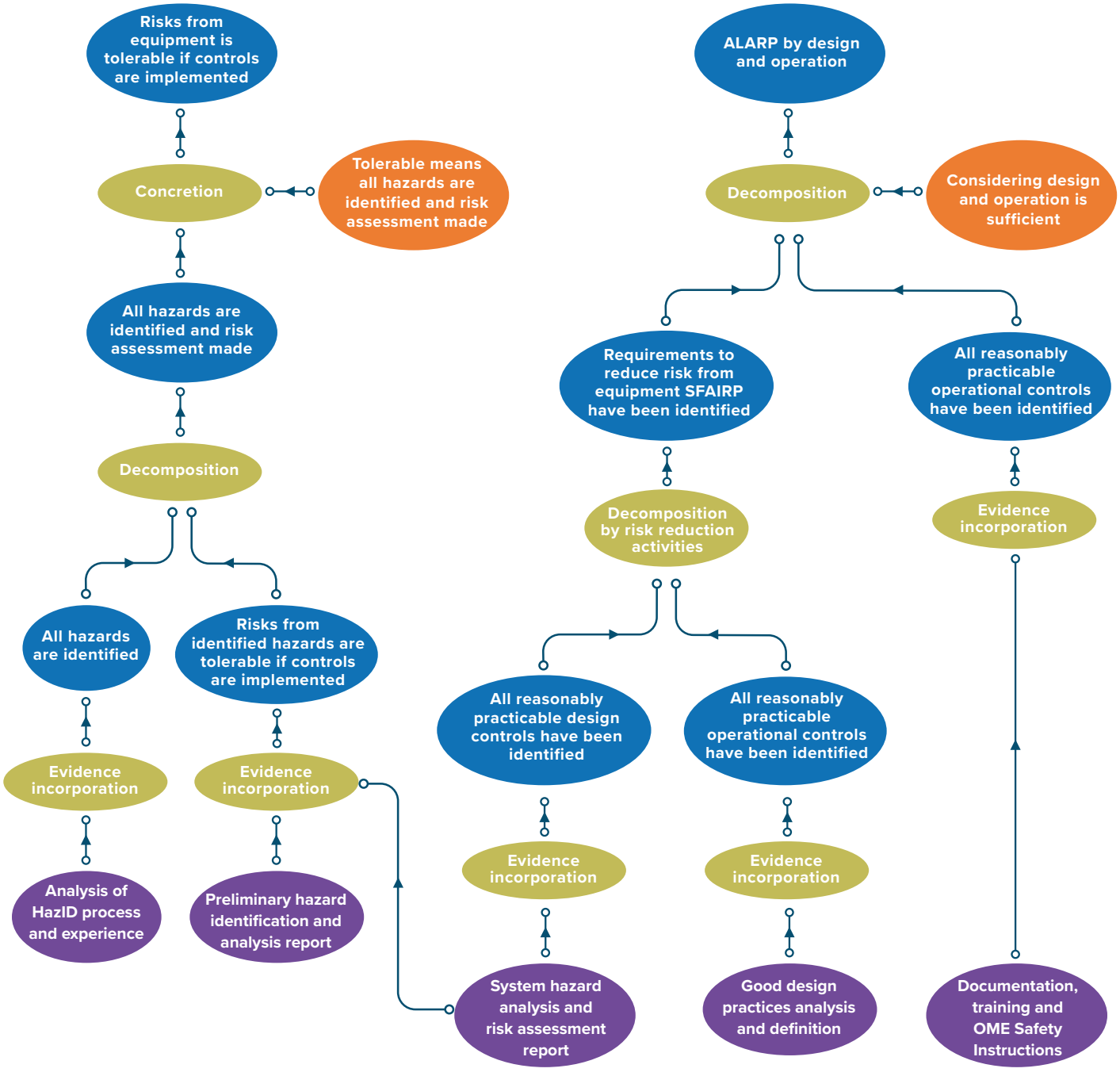

Figure 7: Validity of requirements decomposition

03.
CASE STUDY ANALYSIS

In summary, as requirements and policies are discussed, a CAE structure is created. In doing this the analysis of the policy aspects and safety requirements are developed and some initial results from the risk analysis are produced. Some TRAS comments on evidence identified at L0 are provided in Table 3, where EE is existing evidence, ME – missing evidence, R – recommendations.

Observations from L0 case	TRAS comments
Claims about the system's safety and security requirements assume that some document capturing safety and security requirements exists.	ME: There is currently no single document accumulating all TRAS safety and security requirements. Instead, the requirements are derived from various other documents (high-level requirements, business requirements, safety implications etc.) R: Consider consolidating safety and security requirements into one document.
Claims about the quality attributes of security and safety requirements: requirements should be consistent, unambiguous, unitary, atomic, traceable, verifiable, up-to-date and complete (in the sense that each requirement is fully stated in one place with no missing information) and should be supported by evidence.	ME: At the moment there is no direct evidence dealing with the requirements' quality attributes for TRAS. There could be one report analysing all the quality attributes, or a set of reports combining the analysis of different qualities, outputs from various tools providing natural language analysis of the requirements, etc. R: Develop argument within the safety case for the quality of the requirements. This would consider what is appropriate given the criticality of the system; address the development and approval processes they have been through.

Table 3: Policy and requirements comments on evidence – examples

03.
CASE STUDY ANALYSIS

3.5 SUMMARY OF THE ANALYSIS

To summarise, the application of the overall approach to the TRAS case study started with addressing the first three steps of the cyber security risk assessment process:

Step 1 – Establish system context and scope of assessment

Step 2 – Configure risk assessment

Step 3 – Analyse policy interactions

These guided the development of the L0 assurance case, which concerns requirements, policies and principles of the system and provides the highest level of abstraction in our layered approach.

A summary of the application of Steps 1 – 3 resulting in the L0 case is provided in the tables below.

Step 1	Establish system context and scope of the assessment	Case study
Objectives	Describe the system to be assessed and its relationship with other systems and the environment. Identify the services provided by the system and the system assets. Agree the scope of and motivation for the assessment and identify the stakeholders and their communication needs. Identify the type of decisions being supported by the assessment.	Overview of the TRAS system is provided in Section 3.1. The business requirements and the high-level requirements provide detailed descriptions but these need categorising and prioritising into a service-based perspective.

Table 4: Summary of Step 1 – Establish system context and scope of the assessment

Step 2	Configure risk assessment	Status of case study
Establish safety context	Identify any existing analyses, e.g. safety cases, business continuity assessments that provide details of the system, the impact of failure and the mitigations that are in place. Characterise the maturity of the systems or project and the key uncertainties.	Safety documentation for legacy parts of the system has been identified and the TRAS sponsor is leading work to develop a safety case for TRAS.
Identify threats	Ensure that the risk assessment is focused on the kinds of threats that are of concern. Define possible threat sources and identify potential threat scenarios. Refine generic capability and impact levels for the systems being assessed. Identify risk criteria.	A review suggests that, based on system criticality and infrastructure, attack capability level C is proposed to be appropriate. This is to be confirmed with Government specialists.
Refine and focus system models	Refine and focus system models in the light of the threat scenarios and existing analyses to ensure that they are at the right level of detail for an effective security-informed risk analysis.	The architecture model used in the safety analyses was the result of several iterations. This is presented in Section 3.2 and in ‘Worked example: Architecture and implementation assurance case’.

Table 5: Summary of Step 2 – Configure risk assessment

03.
CASE STUDY ANALYSIS

Step 3	Analyse policy interactions	Status of case study
Identify and define policies and their interaction	Undertake an analysis of policy issues considering interactions between safety requirements and security policies. Resolve any conflicts, show that the trade-offs are satisfactory and document the decisions made. Define additional policies and requirements coming from the analysis.	Some security policies are dealt with in the business requirements. The solution architecture document identifies a variety of security measures, e.g. the backup policy, regular penetration testing. A comprehensive list defining the security policies is given in Section 3.3.

Table 6: Summary of Step 3 – Analyse policy interactions

3.6 DISCUSSION

This real, anonymised example was done to budget and time in a real project.

This example could be augmented with a more detailed use of the CAE blocks. For example, the argument blocks in Figure 5 could be examined and justified by using side-claims (see 'CAE Connection Rules') as the sources of safety and security requirements might be different or benefit from more specific decomposition. Other enhancements might be to use the process set out in 'CAE Review and Challenge' to complete a sentencing statement for the example.

04.
ACKNOWLEDGEMENTS

This document is based on material developed in previous CPNI projects and published research by Adelard.

Disclaimer

This guide has been prepared by CPNI and is intended to support the implementation of security-informed safety assurance and the Claims, Arguments and Evidence (CAE) methodology. This document is provided on an information basis only, and whilst CPNI has used all reasonable care in producing it, CPNI provides no warranty as to its accuracy or completeness.

To the fullest extent permitted by law, CPNI accepts no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the report or arising from any person acting, refraining from acting, relying upon or otherwise using the [report]. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.

No Endorsement

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply its endorsement, recommendation or favour by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

CPNI
Centre for the Protection of National Infrastructure