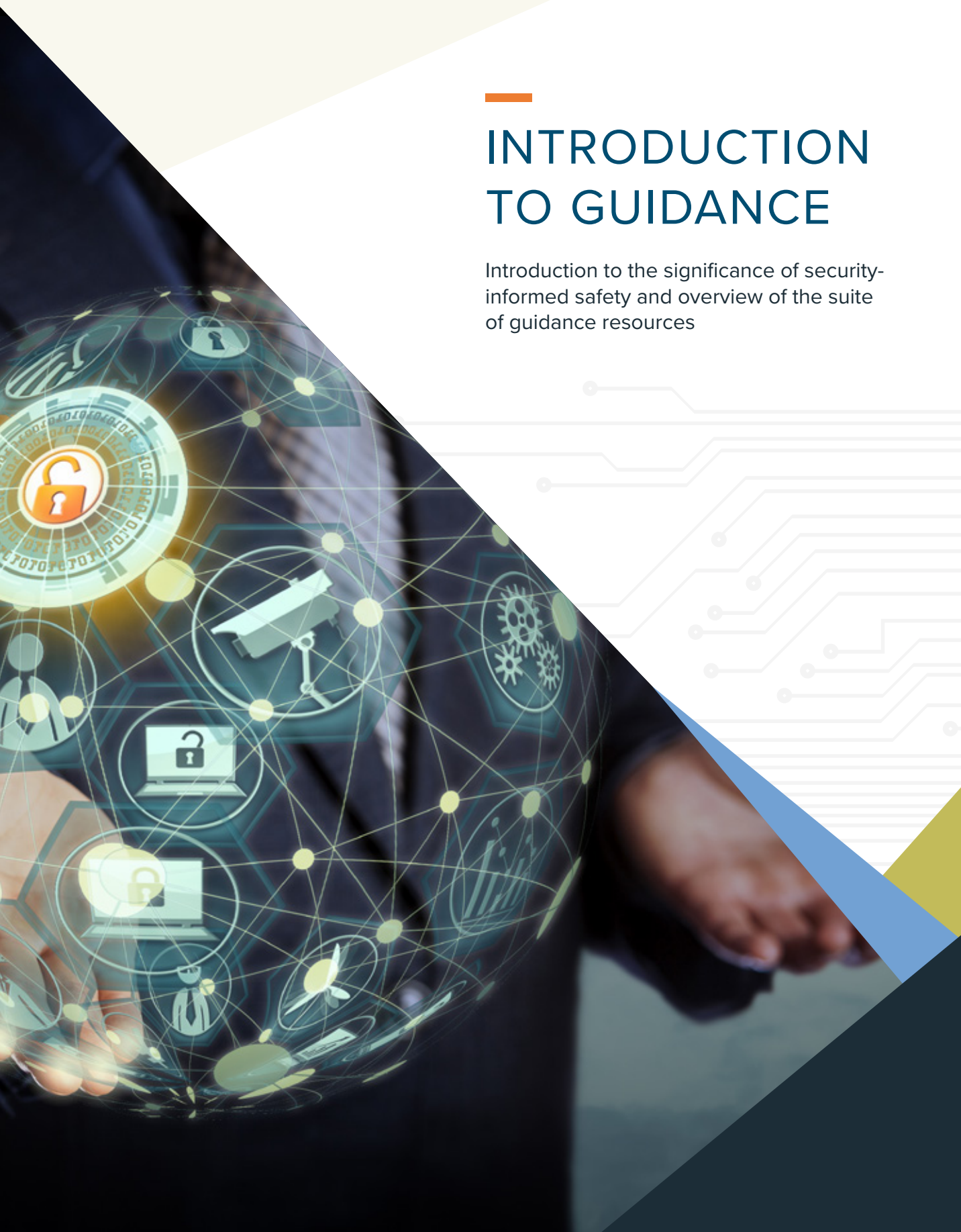
National Protective Security Authority

INTRODUCTION TO GUIDANCE

Introduction to the significance of security-informed safety and overview of the suite of guidance resources



CONTENTS

FIGURES

TABLES

01. INTRODUCTION

This document provides an introduction to security-informed safety and why it matters. It gives an overview of the guidance resources available and includes advice on how to use the guidance documents depending on the area of interest and expertise.

02. SECURITY-INFORMED SAFETY

Society depends on highly connected and complex socio-technical systems. To deliver benefit to society these need to be effective, safe and secure.

Safety can be defined as the state of relative freedom from threat or harm caused by random, unintentional acts or events, while security can be defined as the state of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts.

Safety addresses the harm the system does to the environment, including people.

Security concerns the harm the environment does to the system.

The threats to systems have been increasing and the increased connectivity of systems exposes them to more frequent and different attacks, as well as introducing more complex consequences of failure and interdependencies. We cannot assume that a safety system is immune from attack because it is built using bespoke hardware and software, or because it is separated from the outside world by an air gap.

Security and safety are closely interconnected and interdependent and a safety justification, or safety case, is incomplete and unconvincing without a consideration of the impact of security. This can be succinctly summarised as:

"IF IT'S NOT SECURE, IT'S NOT SAFE".

NPSA recognises the importance of security-informed safety and over the past decade, drawing on academic and industry research as well as sponsoring its own targeted research, has supported the development of a number of industry Codes of Practice and standards, as well as a collection of guidance notes which aim to help government, regulators and industry by:

- identifying the issues and the interdependence between safety and security
- showing how these can be explored from a risk assessment process and a layered assurance case view;
- providing concepts and techniques to help express and communicate understanding of the system risks and their mitigation;
- providing some concrete examples to illustrate the guidance.

In addition, NPSA and the Department for Transport (DfT) have identified future issues arising from artificial intelligence and machine learning (AI/ML) technologies and have undertaken work looking at the specific issues of assuring autonomous systems. This has resulted in a series of Technical Topic Notes that provide technical insights into current research and practices.

03. GUIDANCE RESOURCES

3.1 OVERVIEW

The suite of guidance documents covers extensive information on the approach to security-informed safety assurance and the Claims, Arguments and Evidence (CAE) methodology.

The guidance can be divided into three layers (see Figure 1):

- detailed generic guidance on security-informed safety – the overall approach
- practical illustrative example-based guidance
- a set of generic guides on assurance case concepts and their application that provide the basis for the other guides

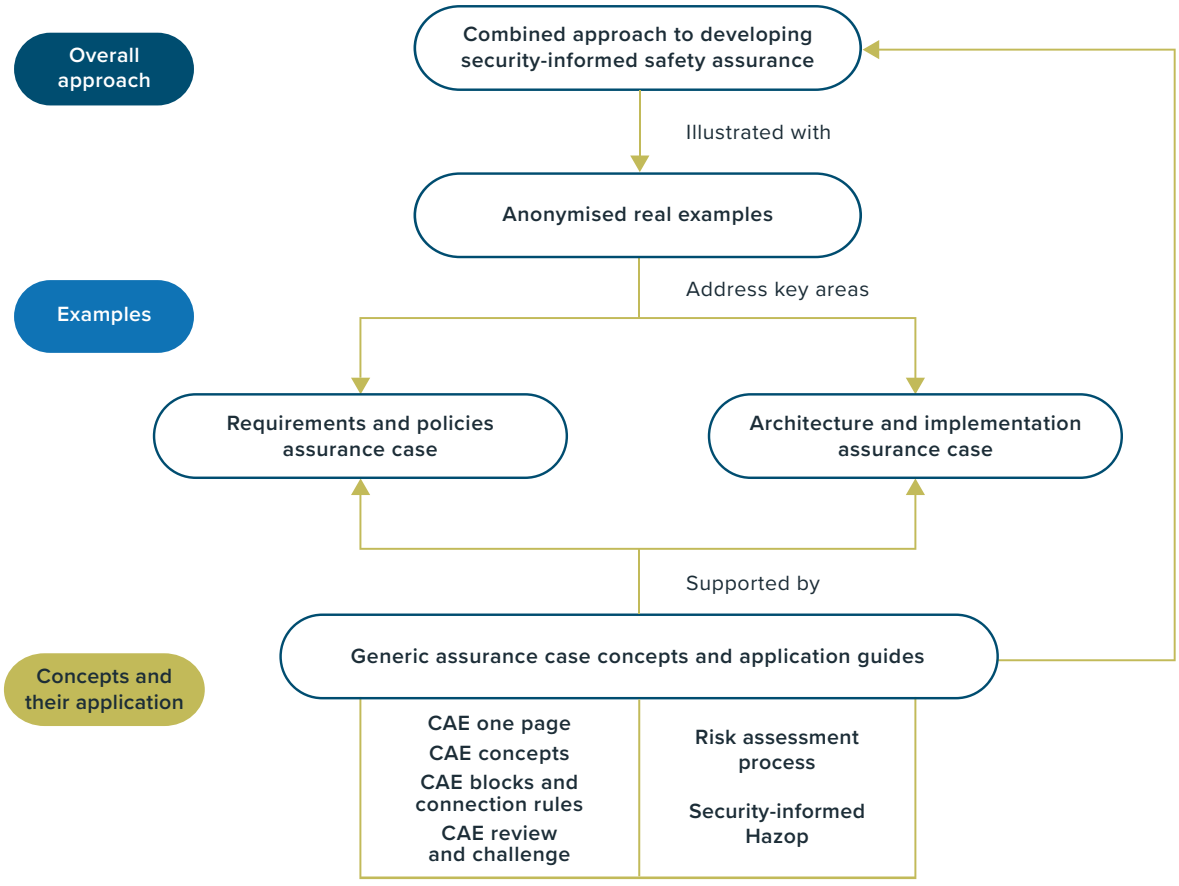


Figure 1: Guidance layers

03. GUIDANCE RESOURCES

3.2 HOW TO USE THE GUIDANCE

Depending on the reader's background and expertise, these guidance documents can be used for different purposes. To facilitate a focused reading and understanding of the guidance, a route through the guides and how they flow sequentially is set out below.

'Combined Approach to Developing Security-Informed Safety Assurance' should be used as an entry point to the overall approach. The document contains an introduction to security-informed safety and gives an overview of the two main components involved in achieving security-informed safety assurance: the development of an engineering cyber security risk assessment process; and a layered assurance case approach.

After gaining an initial understanding of the methodology, readers can refer to the scenario-based examples:

- 'Worked Example: Requirements and Policies Assurance Case'; and
- 'Worked Example: Architecture and Implementation Assurance Case'

for practical guidance on the application of the combined approach illustrated by real anonymised systems. The two example-based guides assume familiarity with the CAE approach, which is covered in detail in the CAE guides.

As described above, the first main component involved in achieving security-informed safety assurance is the development of an engineering cyber security risk assessment process. The 'Risk Assessment Process' guidance provides a more in-depth description of the cyber security risk assessment methodology defined as a series of steps. This guidance document is useful for understanding the process of generic engineering risk assessment and how it is synthesised with information assurance. The guidance can be used to facilitate the comprehension of the scenario-based examples or as supporting material when performing a risk assessment as part of a security-informed safety case.

The second main component is a layered assurance case which defines the abstraction layers of assurance and uses the CAE approach to create a structured case and build confidence in the security and safety properties of a system. The layered assurance is done on the basis of security-informed hazard analysis. The 'Security-informed Hazop' document contains guidance on how to perform hazard analysis. Similarly to the risk assessment guidance, it can be used to enhance the comprehension of the scenario-based examples or as supporting material when building a security-informed assurance case.

Four guides describe the CAE approach, each covering different aspects of CAE in varying levels of detail:

- 'CAE One Page Mini-Guide' – useful as a quick reference point for practitioners who are already familiar with CAE.
- 'CAE Concepts' and 'CAE Blocks and Connection Rules' – can be used by beginners to gain an initial understanding and background to CAE and contains the necessary level of detail required to comprehend the CAE structures in the scenario-based examples.
- 'CAE Review and Challenge' – applicable for practitioners looking to build their own assurance case in CAE or those performing a critical review of an assurance case in CAE.

03. GUIDANCE RESOURCES

3.2 HOW TO USE THE GUIDANCE

Table 1 below suggests a route through the set of guides based on roles and gives rationale on which guides might be applicable to particular roles.

Role	Relevant guides	Rationale
Safety assessor / engineer	Combined Approach to Developing Security-Informed Safety Assurance Risk Assessment Process Security-informed Hazop Worked Example: Requirements and Policies Assurance Case Worked Example: Architecture and Implementation Assurance Case CAE guides	Familiar with safety principles and practices but might not be familiar with CAE methodology and security practices. Will need to have a good understanding of the security-informed safety combined approach and the CAE methodology in order to build or assess an assurance case.
Security assessor / engineer	Combined Approach to Developing Security-Informed Safety Assurance Security-informed Hazop Worked Example: Requirements and Policies Assurance Case Worked Example: Architecture and Implementation Assurance Case CAE guides	Familiar with security risk assessment approach but might not be familiar with CAE methodology and safety principles. Will need to have a good understanding of the security-informed safety combined approach and the CAE methodology in order to build or assess an assurance case.
Project manager	Combined Approach to Developing Security-Informed Safety Assurance Worked Example: Requirements and Policies Assurance Case Worked Example: Architecture and Implementation Assurance Case CAE Concepts	Needs to understanding the overall security-informed safety approach and CAE concepts to ensure the security-informed assurance case follows the best practices. Particular interest in interaction of the requirements and policies as these can be a source of project risk.

Table 1 Roles and relevant guides

03.
GUIDANCE RESOURCES

3.2 HOW TO USE THE GUIDANCE (CONTINUED)

Table 1 below suggests a route through the set of guides based on roles and gives rationale on which guides might be applicable to particular roles.

Role	Relevant guides	Rationale
Service provider/ manufacturer	Combined Approach to Developing Security-Informed Safety Assurance CAE Concepts Security-informed Hazop	Responsible for providing evidence that services and components meet security-informed safety requirements. Need to be familiar with CAE concepts and the combined approach to deliver evidence to the assurance case.
Safety authority	Combined Approach to Developing Security-Informed Safety Assurance Security-informed Hazop Worked Example: Requirements and Policies Assurance Case Worked Example: Architecture and Implementation Assurance Case CAE guides	Responsible for issuing safety regulations and safety certifications. Need to understand the interaction of security and safety via hazard analysis. Familiarity with the CAE concepts especially review and challenge.

Table 1: Roles and relevant guides

Disclaimer

This guide has been prepared by NPSA 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 NPSA has used all reasonable care in producing it, NPSA provides no warranty as to its accuracy or completeness.

To the fullest extent permitted by law, NPSA 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 NPSA. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

National Protective Security Authority