ADELARD

SECURITY-INFORMED SAFETY - SUPPORTING STAKEHOLDERS WITH CODES OF PRACTICE

24 Waterside
44–48 Wharf Road
London
N1 7UX

T +44 20 7832 5850
F +44 20 7832 5870
E office@adelard.com
W www.adelard.com

Authors
Robin Bloomfield
Peter Bishop
Eoin Butler
Robert Stroud

Summary

We describe our approach towards developing two Codes of Practice (CoPs) for "security-informed safety". We explain the overall structure and organisation of the CoPs, and describe our rationale for this organisation. We also provide some insights into the content and style of the CoPs.

This is the pre-publication draft of a paper that was published as the Cybertrust column for IEEE Computer, August 2018 [1].

Contents

Figures

Tables

1 Background

Safety engineering already has a good, but not unblemished, record of providing high technology that is safe and effective. However, the increasing cyber threat and the well documented trend towards more complex and interconnected systems means that change is needed if that record is to continue or improve. We work in a programme that is aimed at changing the way that engineers think, in order to make it common practice for them to consider the impact that their work may have on security, and also the impact that security may have on their work (i.e. 'security mindedness'). Our contribution is aimed at making safety engineers more aware of security, and giving them the processes, procedures and knowledge they need in order to address security in their work. Towards that end, we have developed two Codes of Practice (CoPs) for the rail and automotive sectors, sponsored by government with support from industry stakeholders. We are building on our previous work on security-informed safety [2], which was summarised in a previous IEEE Computer article [3]. The two CoPs are intended to complement and standardize current industry initiatives to create a process for cooperation between security and safety engineers. They are primarily aimed at people with a safety background who need to know how security issues impact on their existing safety practice, but in response to comments from our industry stakeholder group, we have also provided a route through the documents for those with a security background.

2 Scope of CoP

Each CoP applies to the entire rail or automotive transport ecosystem and is intended to be used by suppliers, operators and maintainers of systems used in a connected transport system. The CoPs are intended to help organizations in the transport ecosystem ensure that security-related risks in their products, services or activities do not pose unacceptable risks to safety. Security concerns that are not directly safety-related, such as confidentiality, privacy and theft, as well as financial and reputational risks fall outside the scope of the CoPs.

The CoPs apply to risks that can affect a single system or a few systems. The CoPs also give recommendations for managing systemic risks – wider risks which might appear small, but which become more significant when interdependencies are considered and where the failure of a single or a few entities could result in more widespread failure.

One important aspect of the CoPs is the recognition that every organization within the transport ecosystem should be a 'good citizen' with regard to cyber security in order to minimise the safety risks to users of transport systems and society as a whole

3 Approach

There is already plenty of advice and guidance available on safety and security but it can sometimes seem rather ad hoc. We wanted to adopt a more systematic approach in order to justify the structure and contents of the CoPs and ensure complete coverage of the life cycle.

Our overall approach to developing each CoP was to

- develop a generic set of principles that are applicable to security-informed safety from
  - analysis of existing related principles
  - consideration of the objectives of security-informed safety
  - experience with developing security-informed safety assessments
- adapt these generic principles to the rail and automotive industry by providing appropriate annotations and comments
- provide a set of supporting appendices that include more detail and guidance about the application of the CoP

The initial development of the CoP was undertaken using a combination of 'top-down' and 'bottom-up' approaches.

3.1 Top-down view

To develop and justify the generic principles for the CoP, we constructed a Claims-Argument-Evidence (CAE) case [4] showing how the principles support a high-level vision for industry.

The top-down approach started from an overall vision for the transport sector, for example:

> *"We see a world where everyone has confidence in a safe and secure rail transport sector"*

From this, we derived a top-level claim:

> *"There is justified confidence that cyber security issues do not pose unacceptable risks to the safety and resilience of rail transport"*

Then, using the Claims-Argument-Evidence (CAE) approach to assurance, we developed a network of linked sub-claims supported by a set of principles. These principles were then used to derive the recommendations in the CoP.

The complete CAE structure we developed can be seen in Figure 1, which identifies the main areas of the principles. These include claims about

- current and future organizational aspects
- assets and competencies
- development life cycle
- assurance case
- future behaviour of the product
- supporting confidence of other stakeholders

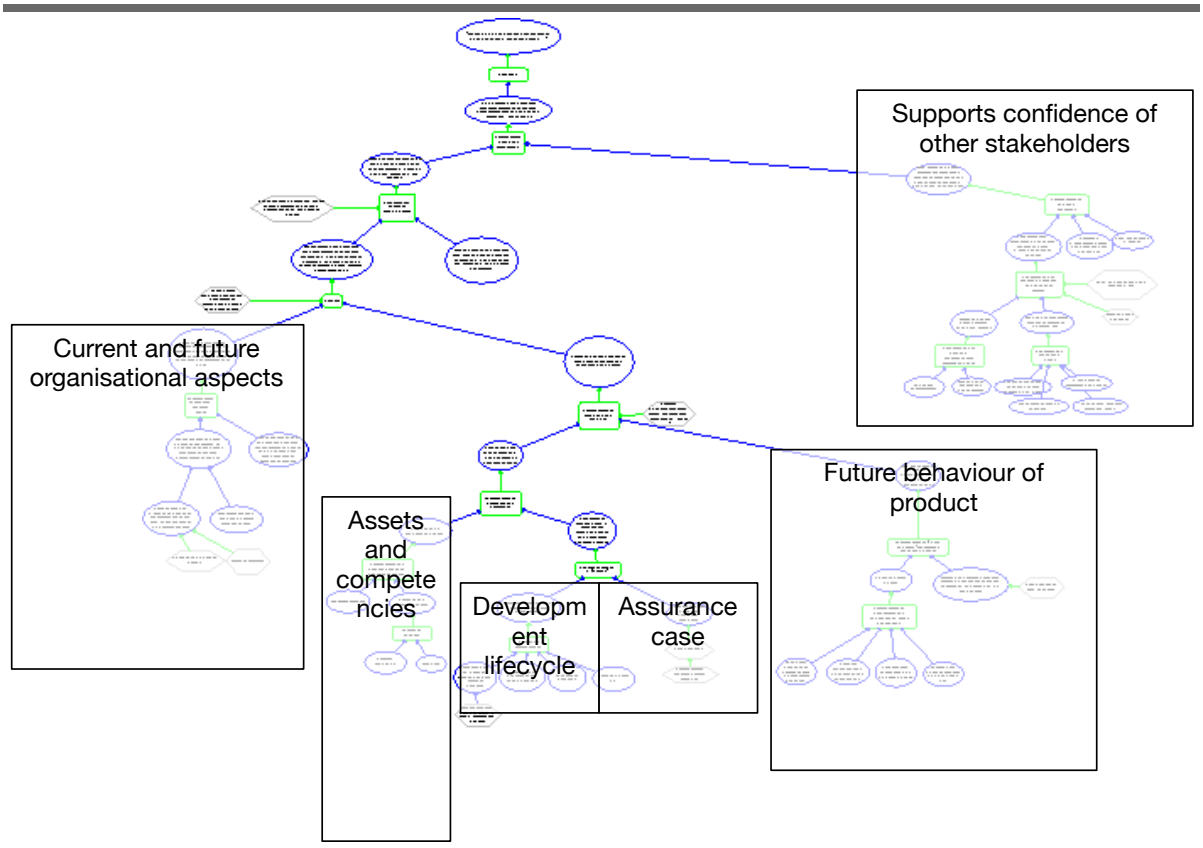

Figure 1: CAE structure

3.2 Bottom-up view

The bottom-up approach started from existing sets of security- and safety-focused principles and guidance produced for a number of safety-related sectors, including:

- **UK Department for Transport (DfT) Centre for Connected and Autonomous Vehicles (CCAV):** The key principles of cyber security for connected and automated vehicles [5]
- **EU Agency for Network and Information Security (ENISA)**: Cyber security and resilience of smart cars – good practices and recommendations [6]
- **US National Highway Traffic Safety Administration (NHTSA)**: Cybersecurity for Modern Vehicles [7]
- **UK National Cybersecurity Centre (NCSC)**: Network and Information Security (NIS) Directive guidance [8]
- **UK Office for Nuclear Regulation (ONR)**: Security Assessment Principles (SyAPs) for the Civil Nuclear Industry [9]

Although none of these documents addressed the exact scope of the project, they were nevertheless all useful sources.

We examined overlaps between these various sets of principles and extracted common themes. These were compared with the initial set of recommendations derived from our 'top-down' approach to ensure that there was adequate coverage of the important points.

Using this bottom-up approach, we identified a set of categories and mapped the various sets of principles onto these categories. Our analysis identified three broad categories of principles:

- organizational security;
- product or project lifecycle;
- design principles (covering architecture through to component design).

3.3 Organization and contents

Based on our top-down and bottom-up analyses, we identified six broad topics that formed the sections of the code of practice, as shown in Table 1.

Section	Indicative contents
1. Security policy, organization and culture	The impact of security considerations on existing safety policy and organizational culture
2. Security-informed development process	Security requirements for each phase of the system life cycle
3. Maintaining effective defences	Ensuring that security is maintained during operation
4. Incident management	Managing security incidents
5. Secure and safe design	Building security into the design of the system
6. Contributing to a safe and secure world	Cooperation and collaboration with other organizations to improve the security of the transport eco system

Table 1: Organization and contents of CoP

Each CoP also contained a number of appendices that provide more detailed guidance on specific topics to help organizations implement the recommendations, as summarised in Table 2.

Appendix	Indicative contents
A. Derivation of principles	Explains how the high level set of principles that inform the CoP were derived
B. Risk assessment	Describes approaches to combining safety and security risk assessment
C. Assurance and safety cases	Provides an introduction to assurance and safety cases
D. System composition	Discusses the challenges posed by systems of systems
E. Network security	Factors to consider in order to determine whether a network is secure – the distinction between open and closed networks
F. Secure coding	Provides an overview of standards and guidance for secure software development

Table 2: List of appendices in CoP

In line with modern regulatory approaches, the recommendations in the CoPs are framed as outcome-based measures, accompanied by notes about the characteristics that adequate implementations of these measures would be expected to have.

4 Example – Contributing to a safe and secure world

An innovative aspect of the CoPs is that they recognise the need for every organization within the transport ecosystem to be a 'good citizen' with regard to cyber security in order to minimise the safety risks to rail users and society as a whole.

In this section, we illustrate the general style and content of the CoP. Each section of the CoP begins with some introductory text that discusses the impact of security considerations on this particular aspect of safety practice. For example, the introduction to this particular section of the CoP (see Figure 2) contrasts the open culture of safety towards learning from accidents and near-misses, with the need to share information about security vulnerabilities in a responsible and controlled way. It also explains that ensuring the security of the ecosystem is a shared responsibility and introduces the concept of 'herd immunity'.

Section 6 Contributing to a safe and secure world

In safety industries, lessons learned are typically shared to push best practice forward. The safety of systems is often communicated to end users and society at large via compliance with regulations, certification to standards, or specific testing schemes. Accident and near-miss investigations provide a formalized route for learning from experience, especially in the regulated high-hazard industries.

In contrast, in a security context, information that might help adversaries to optimize their behaviour needs to be protected. This includes information on vulnerabilities that are in the process of being patched, or details of the organization's threat intelligence or details of both successful and unsuccessful attacks.

It is worth noting that an organization's assets could be used to compromise the assets of another, and the resilience of the transport system as a whole can be improved if all assets involved are hardened against attack – so called herd immunity – and information on security vulnerabilities and failure modes is shared to enable appropriate design decisions to be made. While the safety focused organization will be attuned to the need to monitor, respond and learn from and share experience, security will bring new definitions of what constitutes an event worth reporting, changes to how and to whom this information is reported, the protocols for reporting and escalating externally. This is particularly relevant in the context of systemic failure, where hazardous situations can be caused in a class of systems due to a shared common vulnerability.

Figure 2: Contributing to a safe and secure world – introduction

Following an introduction of this nature, the recommendations for that section are presented, grouped into a series of topic areas. Each topic has a number of clauses that are expressed as outcome-based measures (what should be done, not how it is to be done), accompanied by explanatory notes and pointers to relevant guidance and standards where appropriate.

To continue the example of contributing to a safe and secure world, Figure 3: presents the recommendations in this section, which are grouped into five topic areas.

6.1 Managing risks

6.1.1 The organization should assess and manage risks to

a) the wider transport system
b) society more generally

that might be derived from failure or compromise of its products or services.

NOTE 1: The approach will depend on the safety related nature of the product or service and the regulatory regime that applies.

NOTE 2: Examples of risk to society generally might include the widespread failure of the organization's products and services, leading to a reduction in transport capacity with a consequential impact on many other activities.

6.2 Compatibility and interoperability

6.2.1 The organization's products and services should make use of industry-adopted standards for communication and security, where they can be shown to support adequate levels of safety and security.

6.3 Information sharing

6.3.1 Organizations should enable customers to assess the security of their products and services by making sufficient design and assurance information available.

NOTE: To protect intellectual property, confidential information such as detailed design documentation can be made available under an NDA.

6.3.2 The organization should be able to provide third parties with assurance or certification that the organization's processes relevant to the production of a safe product or service are secure.

6.3.3 The organization should collaborate with relevant organizations to obtain knowledge and understanding of current and relevant threats.

6.3.4 If the organization becomes aware of vulnerabilities that affect or might affect the products or services of another organization, they should responsibly disclose such vulnerabilities to those organizations.

NOTE: Vulnerabilities might be identified through post-incident analysis (see Section 4.5), or reported by third parties.

6.3.5 The organization should support other organizations in the ecosystem to understand and manage security risks arising from the use or abuse of its services or products.

NOTE: Relevant organizations might include governmental organizations (including security agencies), industry umbrella groups and other industry actors.

6.4 Collaboration

6.4.1 The organization should collaborate with relevant organizations to share, develop and foster the adoption of good engineering practices to mitigate current and relevant threats.

NOTE: Relevant organizations might include governmental organizations (including security agencies), industry umbrella groups and other industry actors.

6.4.2 The organization should define an approach for adopting open design practices and deciding when and how to share designs and source code.

6.5 International issues

6.5.1 Organizations should consider the implications of working with organizations from other countries throughout their supply chain. Some countries may harbour malicious intent towards the UK.

NOTE: Further guidance on supply chain risk is available from CPNI [10] and NCSC [11].

Figure 3: Contributing to a safe and secure world – recommendations

5 Achieving a balance between security by design and secure operation

Building systems that are both safe and secure requires a defence-in-depth approach. Ideally, systems should be secure by design. Failing that, they should be operated in a secure environment. Moreover, there should be procedures in place to deal with the possibility of the secure environment being compromised.

The CoP makes a distinction between building systems that are secure and safe by design, and ensuring that systems remain secure and safe during operation. Many legacy systems were designed to operate safely on a closed network but are vulnerable to attack if they are connected to an open network. Such systems were designed to be safe but are not necessarily secure because they assume a benign environment. Since it may not be possible to patch vulnerabilities in a legacy system, the security risk has to be managed. However, new systems should be designed to be secure and safe by default, and should be able to withstand an attack from an adversary that has gained access to a protected network zone. There should also be mechanisms in place to detect the presence of an adversary in the protected network zone and limit or quarantine their access to the rest of the network.

The CoP contains advice and guidance on all of these topics, specifically:

- Security-informed development process
- Secure and safe design
- Maintaining effective defences
- Incident management

6 Discussion and conclusions

The CoPs are not intended to replace existing safety and security standards and guidance, but rather to provide principles and guidance on how organisations can incorporate security considerations into their safety engineering life cycle and become more security minded. One of our goals in writing the CoPs was to keep the core guidance to about 20-30 pages, which we have achieved. The CoPs are structured as a set of high-level recommendations, with notes and references to relevant standards, and appendices that provide more detail on specific technical topics.

Our principled approach to creating a generic CoP that can be adapted to specific sectors such as rail and automotive has been successful. There are relatively few clauses in the CoP that are specific to rail or automotive – most of the advice and guidance is applicable to both sectors.

We currently have mature drafts of both CoPs that are in the process of being reviewed by industry stakeholders before going out for wider public consultation (the road CoP is available from BSI as PAS11281). In order to build consensus around the CoPs, we plan to organise a series of workshops with representative stakeholders to explore the application of the CoP to their situation. We propose that all safety justifications should consider security and an important next step is to show how following the CoP can be used to inform a security-informed safety case.

7 Bibliography

[1] Robin Bloomfield, Peter Bishop, Eoin Butler, Robert Stroud, Security-informed safety – supporting stakeholders with codes of practice, Cybertrust column, IEEE Computer, August 2018

[2] Robin Bloomfield, Kate Netkachova, and Robert Stroud, "Security-informed safety – if it's not secure, it's not safe", in Proceedings of 5th International Workshop on Software Engineering for Resilient Systems (SERENE 2013), Kiev, Ukraine, Oct 2013
https://www.adelard.com/assets/files/docs/Bloomfield_serene_2013.pdf

[3] Kate Netkachova and Robin Bloomfield, "Security-informed safety". IEEE Computer, June 2016.
https://www.adelard.com/assets/files/docs/SIS-paper-v1.pdf

[4] Peter Bishop, Robin Bloomfield, Sofia Guerra, "The future of goal-based assurance cases", in Proceedings of Workshop on Assurance Cases, Supplemental Volume of the 2004 International Conference on Dependable Systems and Networks, pp. 390-395, Florence, Italy, June 2004
https://www.adelard.com/assets/files/docs/dsn2004v10.pdf

[5] HM Government, The key principles of vehicle cyber security for connected and automated vehicles, August 2017
https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles

[6] ENISA, Cyber security and resilience of smart cars – good practices and recommendations, December 2016
https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

[7] National Highway Traffic Safety Administration, Cybersecurity best practices for modern vehicles. Report No. DOT HS 812 333, October 2016
https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf

[8] National Cyber Security Centre, Networks and Information Systems (NIS) Directive: Security objectives and principles
https://www.ncsc.gov.uk/information/networks-and-information-systems-nis-directive-security-objectives-and-principles

[9] Office for Nuclear Regulation, Security Assessment Principles for the Civil Nuclear Industry, v1.0, 2017
http://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf

[10] CPNI, Supply chain
https://www.cpni.gov.uk/supply-chain

[11] NCSC, Supply chain security collection
https://www.ncsc.gov.uk/guidance/supply-chain-security